互普威盾®
ViaControl

用户手册

互普软件
WWW.HUPU.NET

版权声明

版权所有

版权所有 © 2001-2008 上海互普信息技术有限公司。保留所有权利。

本手册之所有咨询皆有版权。本手册之任何资料非经上海互普信息技术有限公司书面同意，不得以电子、机械、磁性、光学、化学、手写或任何之形式加以复制、传送、改写及存储在存取系统，或者翻译成任何语言或电脑语言。

请注意

上海互普信息技术有限公司对本手册内容不做任何担保。上海互普信息技术有限公司对于其中所含的错误，或遵照本手册资讯操作所引起必然或偶然之错误所造成的损害不负赔偿责任。

对于本手册的内容，上海互普信息技术有限公司拥有最终的解释权。

目　录

第一章　简介 1

1.1　前言 1

1.2　功能介绍 2

第二章　安装和部署 4

2.1　基本运行框架 4

2.2　软硬件环境 6

2.3　安装和部署服务器和控制台 7

2.3.1　安装数据库 7

2.3.2　安装服务器和控制台模块 8

2.3.3　服务器注册 8

2.3.4　设置系统检验码 10

2.3.5　服务器日志 10

2.4　部署客户端模块 11

2.4.1　直接安装客户端 11

2.4.2　远程推送客户端 12

2.4.3　域登录脚本安装 14

2.5　系统升级 16

2.5.1　升级服务器和控制台 16

2.5.2　升级客户端 16

2.6　卸载 17

2.6.1　卸载客户端 17

2.6.2　卸载服务器和控制台 17

第三章　控制台 18

3.1　登录控制台 18

3.1.1　登录控制台 18

3.1.2　修改密码 19

3.2 控制台简介 19
3.3 计算机和用户操作 22
3.3.1 查看基本信息 22
3.3.2 分组操作 24
3.3.3 查找 25
3.3.4 删除 25
3.3.5 重命名 25
3.4 控制 26
3.4.1 发送通知消息 26
3.4.2 锁定/解锁计算机 26
3.4.3 注销用户、关闭/重启计算机 26
3.5 辅助功能说明 27
3.5.1 导出和导入 27
3.5.2 打印、打印预览 28
第四章 统计 29
4.1 应用程序统计 29
4.2 上网浏览统计 32
4.3 网络流量统计 34
第五章 日志 37
5.1 基本事件日志 38
5.2 应用程序日志 39
5.3 上网浏览日志 41
5.4 文档操作日志 41
5.5 共享文档操作日志 43
5.6 文档打印日志 44
5.7 移动存储操作日志 46
5.8 资产变更日志 47
5.9 策略日志 48

5.10 系统日志.....48
第六章 策略.....49
6.1 策略简介.....49
6.2 基本策略.....51
6.3 设备控制策略.....54
6.4 应用程序策略.....56
6.5 上网浏览策略.....57
6.6 屏幕记录策略.....58
6.7 日志记录策略.....59
6.8 远程控制策略.....61
6.9 系统报警策略.....62
6.10 流量控制策略.....63
6.11 网络控制策略.....64
6.12 邮件控制策略.....66
6.13 IM文件传送策略.....67
6.14 文档操作策略.....67
6.15 打印控制策略.....69
6.16 移动存储授权策略.....70
第七章 监视.....71
7.1 即时通讯内容.....71
7.2 邮件内容.....72
7.3 实时屏幕.....73
7.4 多屏监视.....74
7.5 查询屏幕历史.....75
7.6 屏幕历史查看器.....76
第八章 远程维护.....78

8.1 远程维护.....78
8.1.1 应用程序列表.....78
8.1.2 进程列表.....79
8.1.3 性能.....79
8.1.4 设备管理器.....80
8.1.5 系统服务.....80
8.1.6 磁盘管理.....80
8.1.7 共享文件夹.....81
8.1.8 计划任务.....81
8.1.9 用户和组.....82
8.2 远程控制.....82
8.2.1 远程控制.....82
8.2.2 远程文件传送.....84
第九章 资产管理.....86
9.1 资产管理.....86
9.1.1 资产类别及资产属性说明.....86
9.1.2 资产类别管理.....87
9.1.3 硬件资产查询.....88
9.1.4 硬件资产变更.....90
9.1.5 软件资产查询.....91
9.1.6 软件资产变更.....91
9.1.7 其它资产.....91
9.2 补丁管理.....92
9.2.1 按补丁模式查看.....93
9.2.2 按计算机模式查看.....94
9.3 漏洞检查.....95
9.3.1 按漏洞模式查看.....95
9.3.2 按计算机模式查看.....95
9.4 软件分发.....96
9.4.1 分发程序包.....96

9.4.2 分发任务 99
第十章 网络接入检测 100
10.1 启动接入检测 100
10.2 启动接入控制 101
10.3 其它设置功能 102
第十一章 数据备份 104
11.1 使用数据库备份 104
11.2 控制台备份及查看 105
11.2.1 备份数据 105
11.2.2 加载和卸载备份数据 106
第十二章 工具 108
12.1 账户管理 108
12.2 计算机管理 111
12.3 警报信息 112
12.4 分类管理 112
12.4.1 应用程序分类 112
12.4.2 网站分类 113
12.4.3 移动存储分类 115
12.4.4 时间类型分类 118
12.4.5 网络地址分类 118
12.4.6 网络端口分类 118
12.5 服务器管理 119
12.6 客户端工具 119
12.7 选项 120
12.7.1 控制台参数设置 120
12.7.2 服务器参数设置 121
第十三章 审计控制台 123

13.1 登录审计控制台 123
13.2 审计界面简介 124
13.3 使用审计控制台 125

第一章 简介

1.1 前言

今天，随着信息科技的高速发展，IT 给企业的运营带来了前所未有的便利，并且逐渐成为企业发展的重要驱动力。但与此同时，IT 也给企业带来了风险和挑战。

企业信息安全隐患激增

现在，越来越多的企业认识到，信息泄漏对企业的危害之重，它不仅给企业带来法律风险、巨额的经济损失，还可能危及企业的生存发展。普华永道与 CIO、CSO 共同举行的全球信息安全调查显示，知识产权盗窃比例为 18%，且雇员首次被列为最有可能制造信息安全事件的因素。

系统应用效率难以评估和控制

最近公布的一项调查结果表明，在工作中使用 MSN、QQ 等聊天的人数高达 89.2%，网页浏览中新闻网页占 65.9%居于首位。一个月薪 2000 元的员工，每天“隐性旷工”2 小时，每年为企业带来的直接损失高达 6000 元。一个拥有 50 人的企业仅此一项每年将损失 30 万。并且滥用网络和系统资源还可能将暗藏于互联网的安全隐患带入企业网络内，威胁系统安全。

系统维护及资产管理繁琐

Gartner 及 Forrester Research 的研究指出，IT 部门接近一半的工作时间用于为计算机安装及升级软件，IT 人员为 PC 做简单的日常维护工作占其总工作量的 70-80%，大大增加计算机网络的综合管理成本。如果问题没有得到及时有效的处理，也会极大影响企业的业务连续性。

Viacontrol 正是一个为企业解决上述问题的有力工具。Viacontrol 运用系统管理思想，充分利用行为审计，分级授权，访问控制和集中管理等技术手段，为企业提供信息安全、应用效率和系统管理的全面解决方案。

1.2 功能介绍

Viacontrol 基于系统管理思想和安全实践经验，全面考虑可能造成信息破坏及外泄的各个方面，保护企业信息不被人为外泄、非法盗取、恶意篡改，帮助企业对信息安全进行系统规划及管理。
Viacontrol 通过灵活有力的管理，在保持企业活力的前提下规范终端行为，提升企业执行力；管理人员通过单一控制台随时了解各台计算机运行状态，并进行系统安全管理及资产管理。

Viacontrol 的主要功能包括：

应用程序管控

记录应用程序使用的日志；
统计应用程序使用时间和百分比；
控制应用程序的运行。

网页浏览管控

记录浏览网页的网址和标题；
统计网页浏览的时间和百分比；
控制访问指定的网站或网页。

文档操作管控

记录所有文档的操作信息，包括不同类型存储设备以及各种文档操作；
记录其他计算机对本机共享目录的删除和修改操作；
可设定灵活的多种操作权限，控制文档的读取，修改和删除操作；
重要文档的复制和删除操作，可对文档进行备份。

打印内容管控

记录所有打印任务的日志；
完整记录文档打印映像；
控制打印操作。

设备管控

控制各种计算机设备的使用；
对任何新增加的设备进行控制。

网络控制

根据客户端类别以及网络地址和端口的类别进行网络通讯控制；
检测网络内的非法计算机，阻止非法计算机接入网络。

网络流量管控

记录网络通讯流量，并按照不同的口径进行统计；
根据不同的地址和端口范围，在不同时间段内实现流量控制。

屏幕监控

实时查看客户端的屏幕快照；
记录客户端的历史屏幕记录，根据不用的应用程序采用不同的记录频率；
可将屏幕历史转换为通用视频文件进行播放。

邮件管控

记录邮件收发的日志以及邮件的完整内容和附件的；
根据策略控制邮件的发送。

即时通讯控制

完整记录流行的即时通讯工具的对话时间，联系人和对话内容；
控制通过即时通讯工具向外发送文档；
对向外发送的文档进行备份。

资产管理

自动扫描每台终端的软硬件资产信息，详尽记录资产变更情况；
可自定义资产属性和类别对软硬件资产和非 IT 资产进行管理；
自动扫描微软产品补丁安装情况，对补丁进行自动分发和安装；
自动扫描客户端的安全漏洞，提供分析报告和解决方案；
自动部署和安装软件、指定程序或派送文档。

远程维护

实时查看客户端的运行信息，可执行远程操作；
远程连接到客户端桌面，进行远程协助；
支持进行远程文件传送。

移动存储控制

记录移动存储设备在网络内的使用，设定不同的访问权限，控制移动存储读取；
对移动存储设备中的文档进行自动加解密，在未经授权的计算机上无法读取。

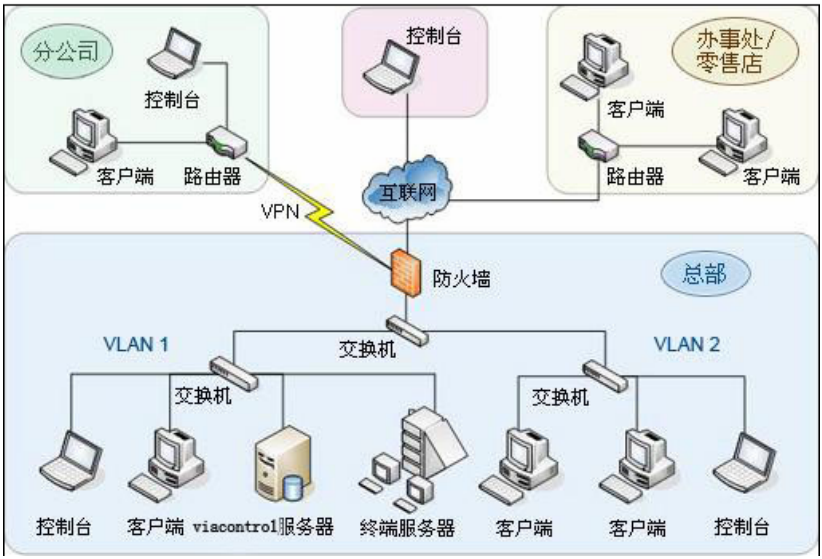
第二章 安装和部署

2.1 基本运行框架

Viacontrol 基本系统由三个模块组成：客户端模块、服务器模块和控制台模块，用户可以根据管理的需要将它们安装在网络中的计算机上。

客户端模块用于收集数据和执行系统管理策略，安装在每台需要被管理的计算机上；
服务器模块用于存储系统数据和管理规则策略，一般安装在性能较高、存储容量较大的计算机上；
控制台模块用于查看系统数据、设定管理策略和进行实时维护，一般安装在企业相关管理人员的计算机上，也可以和服务器模块安装在同一台计算机上。

系统的基本框架如下图所示：



Viacontrol 系统基本架构图

Viacontrol 基于 TCP/IP 协议的网络架构，可以灵活地从本地网络扩展到远程网络和异地网络。服务器通过虚拟专用网（VPN）或互联网连接远程的计算机，实现对大规模复杂网络的集中管理。控制台也可以通过互联网连接异地的服务器，实现对分支机构的远程监控。

服务器模块的基本功能包括：

管理所有客户端计算机，并向其传递相关的规则和指令
收集客户端采集的数据并保存
提供方便灵活的记录管理、查看、归档、搜索等功能

控制台模块的基本功能包括：

查看和审计客户端的数据
数据统计，分析和导出
对客户端计算机实时监控和系统维护
设置监控规则和管理策略

客户端模块的基本功能包括：

执行系统设定的各种管理策略
采集客户端运行的各项数据
定时将采集的数据传送到服务器
根据控制台发出的指令进行监控操作

2.2 软硬件环境

安装 Viacontrol 服务器之前需要先安装数据库，每个模块支持的操作系统以及硬件建议配置如下表：

安装模块	计算机基本要求
数据库	SQL Server 2000 SP4 / MSDE SP4 / SQL Server 2005 SP1 / SQL Server 2005 Express SP1
服务器模块	操作系统 Win2000 SP4 / XP SP2 / 2003 SP1 / Vista 最低配置 Pentium4 2G / 512MB 内存 / 20GB 可用硬盘空间 建议配置 Pentium4 双核或四核 / 2GB 内存 / 60GB 可用硬盘空间
控制台模块	操作系统 Win2000 / XP / 2003 / Vista 最低配置 Pentium III 500/256MB 内存/256MB 可用硬盘空间 建议配置 Pentium4 / 512MB 内存 / 1GB 可用硬盘空间
客户端模块	操作系统 Win98 / Me / NT4 / 2000 / XP / 2003 / Vista 最低配置 Celeron II 433 / 256MB 内存 / 256MB 可用硬盘空间 建议配置 Pentium 4 / 512MB 内存 / 1GB 可用硬盘空间

注意 1. 客户端的某些功能在 Win9x 和 Vista 下不支持;

2. 如果服务器模块安装在 Windows 2000 SP4 系统上，请先确认安装“Windows 2000 SP4 更新汇总升级补丁（KB891861）”。

2.3 安装和部署服务器和控制台

2.3.1 安装数据库

服务器模块的数据库使用 SQL Server 2000 SP4 或以上、SQL Server 2005 SP1 或以上，如果没有 SQL Server 可以安装微软免费提供的 MSDE SP4 或 SQL Server 2005 Express。

如果使用免费的数据库时，建议使用 SQL Server 2005 Express，因为它的容量限制要比 MSDE 大，同时也有自带的管理工具界面，可以比较方便地进行数据库维护。

注意 MSDE 的数据库容量有 2G 的限制，2005 Express 容量有 4G 的限制，而且对服务器的性能也会有一定的限制，所以如果数据量比较大，建议尽量使用 SQL Server 2000 或 2005 标准版（或以上版本）数据库。

安装 SQL Server 2000 请确认安装 SP4 补丁，安装 SQL Server 2005 请确认安装 SP1 补丁。如果导致服务器无法启动，请先在系统的**“计算机管理->事件查看器->应用程序日志”**查看是否属于 SQL Server 版本问题。

SQL Server 2005 Express 的安装

我们推荐安装“SQL Server 2005 Express Edition with Advanced Services”版本。

在安装 SQL 2005 Express 前，操作系统需要先安装：

1. Windows Installer 3.1
2. .NET Framework 2.0

SQL Server 2005 Express 安装步骤：

1) 运行 SQL Server 2005 Express Edition with Advanced Services 的安装程序，接受用户许可协议，并点击【下一步】;
2) 安装 SQL Server 之前需要安装一些组件，单击【安装】按钮安装这些内容，安装成功后单击【下一步】开始 SQL Server 的安装；
3) 单击【下一步】，安装程序会显示必要条件的列表，点击【下一步】继续；
4) 在【注册信息】界面，请注意将【隐藏高级配置选项】勾选项去掉，单击【下一步】继续；

5) 在【功能选择】中请确认已选择【Management Studio Express】；
6) 在实例安装选择时，请确认选择默认的数据库实例（Default Instance），如果选择其他实例，会导致服务器不能正常启动；
7) 设置服务账户时，请选择本地系统账户（Local System）；
8) 之后的设置选择默认值，安装向导将为您完成数据库的安装。

2.3.2 安装服务器和控制台模块

安装数据库完成后，就可以开始安装服务器和控制台了，具体操作步骤如下：

1) 双击 ViaControl3.exe，选择安装界面语言，点击【确定】；
2) 系统会弹出欢迎安装的界面，点击【下一步】继续；
3) 安装程序会提示用户确定安装的路径，用户也可以自己选择安装的路径，可以选择一个存储空间较大的盘符来安装 Viacontrol 服务器；
4) 安装程序会提示用户选择安装类型和组件：用户可以根据需要选择安装 Viacontrol 的服务器和控制台，点击【下一步】；
5) 选择开始菜单的快捷方式的目录，点击【下一步】；
6) 确认设置无误，点击【下一步】，复制文件结束后系统安装完毕，单击【结束】按钮完成安装，服务器模块自动启动，在托盘有个小图标 显示。

安装服务器时，安装程序会判断安装的条件，包括操作系统和 SQL Server 的版本，如果无法正常安装，请按照提示完善安装环境。

管理员也可以在其它机器上单独安装控制台程序，以便查看数据和监视客户端机器的操作。

2.3.3 服务器注册

第一次安装服务器后，Viacontrol 会自动生成一个有 30 天试用期的演示序列号，它是由 6 组 4 个字符组成的字符串。右键单击【服务控制器】，选择“**工具->**

注册”输入管理员密码进入注册界面。

管理员点击【升级】按钮，序列号一栏会变为可编辑状态，输入购买的正式序列号，再单击【确定】按钮，如果您输入的序列号无误，系统会提示“**序列号升级成功**”并且提示您需要激活产品。您必须通过产品注册得到注册码来激活您的产品。

注意 您必须在输入正式序列号以后 15 天内注册您的产品，否则系统将无法继续运行。

如果 Viacontrol 所在服务器可以连接互联网，有 2 种注册方法：

在线注册

在产品注册对话框中填写您公司的信息，包括公司名称、联系人、联系电话和邮件地址，点击【在线注册】会自动返回注册码，单击【注册】按钮，提示“**注册成功**”即可；

邮件注册

您也可以使用邮件注册。在产品注册对话框中填写您公司的信息，包括公司名称、联系人、联系电话和邮件地址，点击【发送邮件】，系统会弹出发送邮件窗口，请确认填写信息无误后发送邮件。
我们会将注册码发到您填写的电子邮件地址，收到后请将注册码复制到相应地方，点击【注册】按钮，系统提示“**注册成功**”就完成了整个注册的过程。

如果因为网络或别的问题，无法在线注册或即时发送邮件获得注册码，您也可以在其他可上网的机器上将注册信息和识别码发送邮件给我们进行处理。

注意 第一次注册时填写的电子邮箱地址是非常重要的，以后因其他原因需要再次注册时，新的注册码我们仍然会发到第一次注册时填写的电子邮箱内。

2.3.4 设置系统检验码

检验码是服务器和客户端除了序列号外唯一的识别码，其目的是增加系统内的安全性。服务器上的检验码必须和客户端的检验码一致，该客户端才能被服务器所管理。所以建议您先在服务器上设置检验码，再打包客户端安装程序，这样就会把服务器的序列号和检验码一起打包到客户端安装程序，防止外来非法的服务器接管企业内的客户端。

当第一次安装服务器后，右键单击【服务控制器】选择菜单“**工具->检验码**”，系统会要求输入管理员的账号和密码，才能设置检验码。输入检验码，再次输入，点击【确定】按钮，设置检验码成功。

系统默认检验码为空，如果客户端没有检验码，第一次设置检验码后，服务器会自动更新所有连接上的客户端的检验码，使客户端的检验码与服务器保持一致。

如果服务器再次设置新检验码，只要客户端识别到服务器之前设置的检验码中有一个与客户端现在的匹配，客户端就会主动将检验码更新为服务器现在的检验码。

警告 管理员请务必牢记自己设置的检验码，以便服务器重装之后或者换了系统后可以顺利接管以前的客户端，否则您可能需要重新部署客户端。

如果发现客户端有运行但是无法在控制台显示，请在 Viacontrol 控制台“**日志->系统事件**”中查看是否属于检验码验证失败的问题。

2.3.5 服务器日志

右键单击【服务控制器】选择菜单“**工具->日志**”会自动链接到操作系统的【事件查看器】。选择【应用程序】可以查看 OSERVER3 的运行日志，包括：服务器程序的启动和停止、错误日志等。管理员通过这些日志信息可以分析服务器的运行情况。

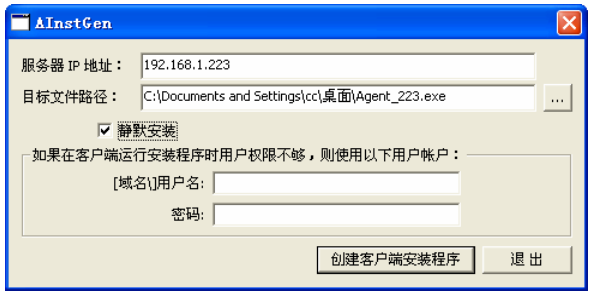
2.4 部署客户端模块

客户端模块的部署有多种方式：直接安装、远程推送、域登录脚本安装，您可根据实际需要完成对客户端机器的部署。

2.4.1 直接安装客户端

直接安装客户端模块需要首先创建客户端安装程序，然后到需要部署的机器上手工运行安装程序，安装客户端程序需要管理员权限。

客户端安装程序需要在服务器机器上打包。在安装了 Viacontrol Server 的机器，点击“**开始->所有程序->Viacontrol V3->创建客户端安装程序**”打开客户端生成工具，出现下图界面。



客户端安装程序的参数包括：

名称	说明
服务器 IP 地址	系统默认是当前计算机的 IP 地址，如果服务器有多个 IP 地址，请输入一个有效 IP 地址。
目标文件路径	客户端安装程序的文件名以及存放路径。
静默安装	选中该复选框，客户端安装程序为静默安装，没有安装界面；不选中该复选框，则为非静默安装包。
用户名和密码	安装客户端需要管理员权限，如果计算机上登录的用户是 user 权限，可能会无法成功安装，这种情况下，可以在创建客户端安装包时，在这里输入具有计算机管理员权限的用户名和密码，这样创建的客户端在 user 权限下也能安装成功。

点击【创建客户端安装程序】按钮，客户端安装程序创建成功。

2.4.2 远程推送客户端

对于较大的企业，计算机数量较多，分布的较广，不方便在计算机上进行手工安装，逐台计算机进行安装也会消耗大量的精力。此时，我们可以通过远程安装的方式来解决这个问题，既可以批量安装客户端程序，也省去了亲自到该计算机上安装的麻烦。

在安装了 Viacontrol Server 的机器，点击“**开始->所有程序->Viacontrol V3->远程安装客户端模块**”运行远程安装工具。

该工具只能对 Windows NT 4.0/2000/XP 的机器进行安装，要安装 Windows 9x/ME 的计算机请直接在所需的计算机上安装。

扫描设置：

系统默认扫描本网段内的所有计算机，如果需要扫描其它网段的计算机，请选择菜单“**文件->扫描设置**”打开扫描设置对话框，添加其它网段的 IP 范围，也可以对扫描包的时间间隔进行设置。

在计算机列表中各种图表代表的含义：

图标	颜色	Window NT4 / 2000 / XP	Window 95 / 98 / Me	是否在线	是否安装 Agent
	深蓝	是	否	是	否
	深蓝	否	是	是	否
	灰色	是	否	否	否
	灰色	否	是	否	否
	浅蓝	是	否	是	是
	浅蓝	否	是	是	是

远程推送

选择需要安装客户端模块的计算机，可同时选择多个计算机，点击“**操作->开始安装**”开始客户端模块的安装，在安装状态栏可以查看每台计算机的安装状态，在下面的安装日志窗口可以查看所有计算机的安装日志。

【常见问题】

- ✧ 当前登录的用户没有操作目标计算机的权限，此时会弹出一个安装出错的窗口，请输入具有目标计算机管理员权限的用户名和密码;
- ✧ 目标计算机没有打开 admin 共享，这时需要到目标计算机上开启 admin 共享，打开命令提示符 cmd.exe，net share 查看 ADMIN$共享是否开启，如果没有打开，net share ADMIN$ 打开 admin 的共享;
- ✧ 目标计算机无法访问本机共享文件，可能是本机的 admin 共享没有打开，目标计算机没有权限访问本机共享文件。

注意 由于 Windows NT 网络内部的一些安全权限的设定影响程序正常运行，所以可能某些时候并不能使您有足够的权限在远程的计算机上执行远程安装。在这种情况下，请您用 Viacontrol 客户端的安装程序到所需的计算机直接安装。

2.4.3 域登录脚本安装

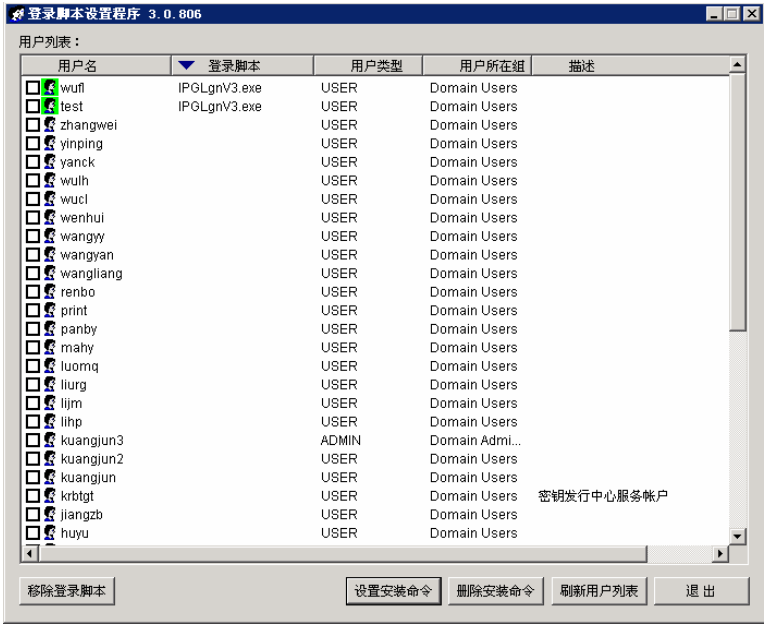
如果网络中有域环境，可以通过修改域脚本来安装客户端。通过修改登录脚本，Windows 用户登录域时，执行登录脚本，将 Viacontrol 客户端安装到本机上。

具体步骤如下：

1) 在安装光盘中找到 LogonScript 目录，将整个目录复制到域服务器机器上；
2) 在 Viacontrol 服务器上创建客户端安装程序，并命名为 ASetup.exe；
3) 将 ASetup.exe 复制到域服务器上的 LogonScript 目录下；
4) 运行域服务器上 LogonScript 目录下的 LgnManV3.exe 程序进行域登录脚本的设置。

使用说明：

1) 运行 LgnManV3.exe 后出现以下的界面，LgnManV3.exe 会自动扫描并排序显示域服务器上的用户信息列表，显示各个用户的登录脚本状态。其中，用户图标底色为绿色表示该用户的登录脚本已经包含我们的安装命令。



2) 管理员可以点击列表表头进行排序，并结合 CTRL， SHIFT 等键选择多个用户，右键“选择”或“取消选择”多个要操作的用户，进行设置安装命令、删除安装命令、移除登录脚本等操作。

3) 设置了登录脚本的用户在登录域时，相关的域脚本将会运行，Viacontrol 客户端会自动安装到指定用户的计算机。

4) 当 Viacontrol 客户端成功安装到所需的计算机，你可以将有关用户的登录脚本还原为原来的登录脚本。

功能按钮说明

功能按钮	说明
设置安装命令	将在选定用户的登录脚本中添加我们的安装命令。
删除安装命令	将在选定用户的登录脚本中删除我们的安装命令。
刷新用户列表	将重新扫描所有用户的信息并显示到用户列表中。
移除登录脚本	将选定用户设置为没有登录脚本（不会删除脚本文件）。
退出	退出该程序。

其它说明

本程序可以设置用户登录不调用脚本，但是不会删除实际的文件，用户必须手动清理不需要的脚本文件。但是请切记在手动删除文件时确认没有任何脚本文件调用该文件。

2.5 系统升级

2.5.1 升级服务器和控制台

升级服务器和控制台可以通过升级包来完成，也可以直接覆盖安装 Viacontrol 安装程序到原来的目录，升级服务器和控制台的具体步骤如下：

1) 运行升级程序，列表中会显示当前版本和升级版本，单击【升级】按钮进行升级；
2) 手工启动服务 OCULAR V3 SERVER 和 OCULAR V3 UPDATE（如果直接覆盖安装，不需要手工启动）

2.5.2 升级客户端

服务器升级成功后，会自动将客户端升级文件传给每个连接上来的客户端，但是需要客户端机器重启才能升级成功。

2.6 卸载

2.6.1 卸载客户端

对于不再需要安装客户端模块的计算机，管理员可以将客户端模块卸载，卸载客户端有 2 种方式：

控制台卸载

选择“**控制->卸载客户端**”将客户端模块移除，此后客户端模块不再运行，如果您以后需要在该计算机上再运行客户端模块，必须重新安装。

客户端工具卸载

对于离线状态的客户端机器，也就是无法与服务器连接的客户端机器，我们提供了另外一种卸载客户端的方法，具体步骤如下：

1) 在客户端机器的“**开始->运行**”中输入命令“agt3tool ocularadv”，打开客户端工具；
2) 选择“**卸载客户端**”，点击【生成操作码】按钮；
3) 会弹出一个“**检验操作码**”对话框，请把原始操作码报告给管理员；
4) 管理员在控制台“**工具-客户端工具-确认码生成器**”输入客户端的操作码，会解析出该客户端的操作以及相应的客户端信息；
5) 管理员确认后点击【生成确认码】；
6) 管理员将确认码告诉客户端，输入正确的确认码执行指定的操作。

注意 卸载客户端和删除客户端的区别：卸载客户端仅仅是移除客户端模块，并不减少 license 数，在控制台上可以显示该计算机并查看日志；而删除客户端包括卸载客户端和减少 license 数。

2.6.2 卸载服务器和控制台

首先关闭 Viacontrol 服务器和控制台等应用程序，然后选择“**开始**”菜单的“**所有程序->Viacontrol V3->卸载 Viacontrol V3**”进行卸载，也可以选择在“**控制面板->添加/删除程序**”中选择 Viacontrol3 进行卸载。

第三章 控制台

3.1 登录控制台

3.1.1 登录控制台

单击安装目录下的 OConsole3.exe 或者“开始->所有程序->Viacontrol V3->Viacontrol V3 控制台”启动控制台模块。
在启动控制台模块之前必须先在网络上运行服务器模块，控制台模块在启动后会显示登录窗口。

登录的对话框中包含以下内容：

字段	说明
服务器	输入服务器的 IP 地址或计算机名称；
账户	初始时预设了系统管理员为“admin”，系统审计员为“audit”，管理员也可以根据不同的权限设置多个管理员账户，在“**工具->账户**”中添加；
密码	管理员的初始密码均为空，登录控制台后可以修改管理员密码，在“工具->修改密码”中修改密码，管理员需要保管好自己设置的密码。

当需要重新连接服务器或者连接到其它的服务器，或需要以不同的管理者身份

进入控制台时，可以选择“**工具->重新登录**”功能重新登录控制台。

3.1.2 修改密码

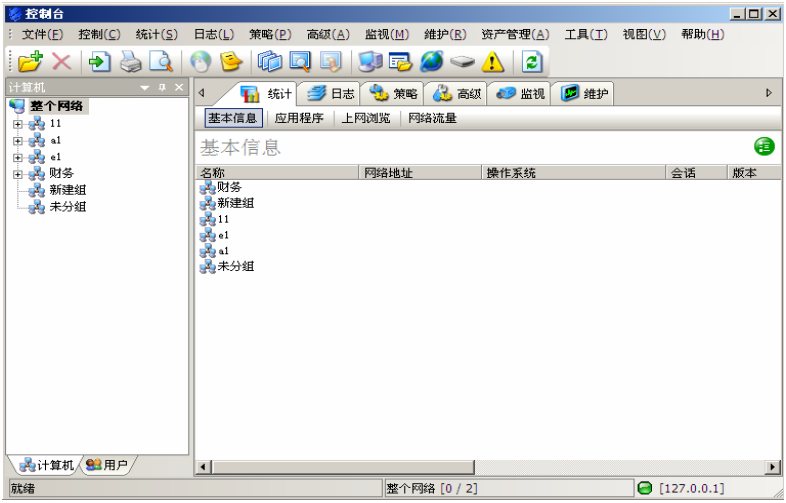
为了保密，用户可以修改自己的密码，以防止他人盗用您的用户帐号登录到系统中执行非法的操作。

登录控制台后，选择“**工具->修改密码**”打开修改密码对话框。输入旧密码，再输入新密码，并在密码确认框中再输入一次，保证两次输入的密码一样，单击【确定】，修改密码成功。注意这里的修改密码只能对当前登录的管理员用户密码进行修改，在这里的第一行会显示当前登录控制台的帐户。

经过服务器模块认可后新密码就生效了。

3.2 控制台简介

控制台登录后，将见到如下的界面视图：



控制台界面包括：

界面区域	说明
菜单栏	包含了本系统的所有菜单，是各功能窗口的入口；
工具栏	包含了一些常用的功能；
计算机栏	位于窗口的左边，显示所有安装了客户端的计算机列表和以及分组信息；
用户栏	位于窗口的左边，显示所有客户端机器登录的用户列表以及分组信息；
导航主菜单	位于工具栏的下方，可以快速导航主要功能；
导航子菜单	对导航主菜单的补充，快速导航到具体的功能；
功能按钮区	位于导航子菜单的下方，该视图也包含了当前功能的标题，功能按钮在标题的右侧；
数据显示区	是本系统的核心视图，所有的数据都在数据显示区查看；
图表栏	只有统计功能包含图表栏，是显示统计图的区域；
查询栏	在统计、日志、即时通讯、邮件记录中均有查询栏，并且有一些通用查询条件，在下面详细说明；
属性栏	只有策略控制功能中包含属性栏，是设置策略属性的区域；
状态栏	位于窗口的最下方，显示当前功能的状态信息。

计算机栏中各图标的含义

图标	颜色	含义
	亮蓝色	客户端模块正常运行
	灰色	客户端模块没有运行，可能是该计算机没有开机或没联网，也可能是防火墙阻断了通讯
	深灰色	客户端模块已被卸载
	亮蓝色带小时钟标志	客户端模块正常运行，但客户端的使用者离开

用户栏中各图标的含义

图标	颜色	含义
	亮蓝色	该用户的客户端模块正常运行

	灰色	该用户的客户端模块没有运行，可能是该用户没有登录

系统通用的日志属性和查询条件

在日志记录中（包含各种事件日志、邮件日志、即时通讯日志），会包含一些通用日志内容：

字段名称	说明
时间	记录该日志的详细时间；
计算机	记录该日志属于的客户端机器，这里的计算机是指在计算机栏中显示的名称；
用户	记录该日志发生的用户，这里的用户是指用户栏中显示的名称。

对于日志和统计数据，我们的通用查询条件包括：

查询条件	说明
时间范围	指定查询的时间范围， 默认起始时间和终止时间都不勾选，也就是查询到所有日志数据。要查询一段时间内的日志，勾选起始时间和终止时间并设置时间范围。
	单击该图标直接查看上一时间段的日志，一个时间段可以是一天、一个星期、一个月等，取决于当前设置的起始时间和终止时间；
	单击该图标直接查看下一时间段的日志，也是取决于设置的时间范围；
	单击该图标自动恢复到系统默认的时间范围。
时间类型	在“**工具->分类管理->时间类型**”中系统预定义了工作时间、休息时间和周末时间，管理员需根据实际情况修改这些时间类型，并可以自定义时间类型进行查询；
范围	单击右边按钮打开范围选择窗口，可以选择单个计算机或单个组(包括整个网络)进行查询。

3.3 计算机和用户操作

3.3.1 查看基本信息

选择菜单“**统计->基本信息**”，管理员可以查看计算机、计算机组、用户、用户组的基本信息。

1) 计算机基本信息

在计算机栏中选择一台计算机，在数据显示区会显示该计算机上客户端模块的运行状态：

字段名称	说明
名称	客户端在计算机树中显示的名称，为了方便管理，该名称可以更改。如果不更改，名称和计算机名称相同；
计算机	客户端所在计算机的真实名称；
网络地址	计算机与服务器通讯的 IP 地址；
状态	客户端的运行状态，包括：正在运行、离线、客户端已被卸载；
版本	客户端的版本号；
操作系统	客户端所在计算机的操作系统版本；
开机时间	当前客户端的启动时间，只有客户端状态为“正在运行”才有该字段；
最后在线时间	客户端最后一次与服务器的通讯时间；
最后活动时间	显示客户端机器的最后活动时间；
安装时间	该版本客户端的安装时间；
IP/MAC 地址	该计算机的所有网卡的 IP/MAC 地址；
最后登录用户	该计算机的当前登录用户，空闲和锁定的状态也会在这里显示。

如果计算机登录多个用户，在最后登录用户的下方，控制台会显示该计算机当前登录的所有用户及登录时间。

2) 计算机组基本信息

在计算机栏中选择一个计算机组，在数据显示区会显示该组下所有的计算机和组的状态列表。

如果选择整个网络，会显示所有的计算机组，单击数据显示区右上角的【展开】按钮“ ”，可以查看这些组下所有计算机的状态列表。

3) 用户基本信息

在用户栏中选择一个用户，在数据显示区会显示该用户的运行状态。

字段名称	说明
名称	客户端在用户树中显示的名称，为了方便管理，该名称可以更改。如果不更改，名称和用户名称相同；
用户	客户端所登录的用户的真实名称，如果是本地系统用户，即显示该用户名；如果是域用户，即显示为域名\用户名；
状态	客户端的运行状态，包括：在线，离线等；
最后在线时间	客户端的在线更新时间；
最后活动时间	客户端所在的用户的活动更新时间；
最后登录的计算机	该用户最后登录的计算机。

如果该用户在不同的计算机上登录，在最后登录计算机的下方，控制台会显示该用户登录的所有计算机和登录时间。

4) 用户组基本信息

在用户栏中选择一个用户组，会显示该组下所有用户和组的状态。同样在整个网络下，单击数据显示区右上角的展开按钮“ ”，可以查看所有用户的状态信息。

3.3.2 分组操作

在计算机栏和用户栏中，所有的客户端机器和用户在首次出现时，默认都会在【未分组】内。为了方便管理，管理员可以新建一些分组，将这些计算机和用户在逻辑上划分到不同的分组中。

新建分组

在计算机栏，选择整个网络或某个分组，选择菜单“**文件->新建组**”，则会在计算机树中出现一个新的组结点，为可编辑状态，输入组名称，将相关的计算机拖到该计算机组。管理员可以按照相同的办法建立多级的分组机构。

切换到用户栏，可以按照相同的方法对用户进行分组管理。

提示 计算机组和用户组都有一个默认分组 “**未分类**”组，新出现的计算机和用户都被归类为“**未分类**”组。“**未分类**”组不能删除，不能重命名，也不能在“**未分类**”内新建子组。

指定分组和改变分组

当需要为计算机和用户指定逻辑的分组时或改变分组时，我们可以选定需要移动的计算机和用户，选择菜单“**文件->移动到**”，选择相应的目标组，这样我们所选择的计算机和用户会移动到我们指定的组内。

我们也可以通过鼠标的拖拽操作来完成。选择我们要操作的对象后，按住鼠标左键不放，然后把它拖到我们所希望的目标组中去，这样我们所选择的计算机(组)或用户(组)就会属于我们指定的组了。

提示 为了方便分组，可以同时拖动多个计算机或用户到指定的分组，如选择“未分组”，查看“统计->基本信息”，按住CTRL或SHIFT键，选择多个计算机或用户到指定分组。

3.3.3 查找

通过查找功能，管理员可以快速定位到指定的计算机或用户，并且查看其相关的数据内容。

查找计算机

在计算机栏中选择“**文件->查找**”打开查找对话框。输入查询条件，查询条件可以是计算机名称（包括在计算机栏中显示的名称和真实的计算机名称），也可以是计算机的 IP 地址，支持模糊查询。

查找出来的计算机在下面的列表中显示，双击其中一台计算机可直接跳转到该计算机的数据显示画面。

查找用户

从计算机栏切换到用户栏，选择“**文件->查找**”，打开查找对话框。输入查询条件，查询条件支持用户名称，包括管理员自定义的用户名和真实的用户名，支持模糊查询。

和查询计算机的操作相同，双击结果列表中的用户可以直接跳转到该用户的数据显示画面。

3.3.4 删除

对于不再需要接受管理和查看其以往数据内容的计算机，可以在控制台上将其删除。选择“**文件->删除**”，可以把计算机栏或计算机列表中选中的计算机(组)删除，如果是计算机组，则包括该组中所有的子组和计算机。删除操作会卸载该计算机上运行的客户端，并且收回相应的 License 授权；

删除用户(组)只是删除用户的信息，并不影响 License 授权。当该用户再次登录后，系统仍然会出现该用户的信息。

3.3.5 重命名

为了方便管理，管理员可以将计算机名称或用户名称改为便于管理和查看的名称。选择要更改名字的计算机(组)或用户(组)，选择菜单“**文件->重命名**”进行改名，修改后的名称将会显示在控制台上。

3.4 控制

管理员可以通过控制台对运行客户端模块的计算机进行控制，前提是所要进行控制的计算机必须正在运行客户端模块。控制只能针对计算机，在用户模式下不能进行控制。

3.4.1 发送通知消息

当需要对客户端用户发送一些通知消息或下达某些命令时，可以直接通过控制台的发送通知消息功能进行通知。

选择目标客户端机器或组（如果是组，则对组内所有计算机发送通知消息），选择菜单“**控制->发送通知消息**”打开一个对话框，输入通知的内容，点击【发送】按钮。目标计算机的桌面将会弹出通知消息窗口。

3.4.2 锁定/解锁计算机

当发现运行客户端模块的计算机有异常举动或有其它原因时，管理员可以将该计算机或多个计算机进行锁定，阻止用户继续使用键盘和鼠标进行操作。

选择菜单“**控制->锁定计算机**”进行锁定。被锁定的计算机将无法再使用键盘和鼠标进行任何操作，只有对它进行解锁，用户才能继续使用键盘和鼠标。被锁定的计算机在基本信息里面会显示锁定的状态。

当需要对已锁定的计算机解锁时，选择菜单“**控制->解锁**”进行解锁，目标计算机就可以继续使用键盘和鼠标了。

3.4.3 注销用户、关闭/重启计算机

当需要关闭运行客户端模块的计算机，可以使用此项功能。管理员可以选择“**控制**”菜单的“**注销用户**”、“**重新启动**”和“**关闭计算机**”执行相应的操作。目标计算机会执行控制台下达的命令。当然执行此操作后该客户端模块将退出直到下次重新登录后才会开始运行。

3.5 辅助功能说明

在控制台的使用中，还有一些其它的通用功能，在很多功能模块中都会用到，下面将做简单说明。

3.5.1 导出和导入

数据的导出

控制台上的所有数据视图均可以导出保存为电子文档，包括：统计、日志、策略、即时通讯内容、邮件内容、资产管理等等。部分模块的导出可能会有细微的差别。

导出本页记录

在数据视图中单击右键“**导出->导出本页记录**”只会导出当前页的日志，默认是 20 条记录，管理员可以在控制台“**工具->选项->控制台设置->日志查看**”中修改每页显示的最大记录数；

导出所有满足条件的记录

在数据视图中单击右键“**导出->导出所有满足条件的记录**”会导出所有记录。导出的文档可以保存为 3 种格式：文本文件(.CSV)、HTML 文件、EXCEL 文件（前提是机器安装了 Microsoft 的 Excel 程序）。

策略的导出/导入

只有策略模块提供导入功能，策略的导出/导入是为了方便管理员设置策略。

选择需要导出的策略，单击右键“**导出**”或“**导出选中的策略**”保存为 xml 格式文件，“**导出**”是导出当前所选计算机(组)或用户(组)的当前模块的所有策略，不包括继承的策略。“**导出选中的策略**”只导出其中选中的策略，可以是一条，也可以是多条。

选择需要导入策略的计算机(组)或用户(组)，单击右键“**导入**”选择策略文件导入策略，保存生效。导入的策略必须与当前的策略类型一致，否则无法导入。

3.5.2 打印、打印预览

控制台上的所有数据视图均可打印出来存档，留作日后参考。选择菜单**“文件->打印”**，用户可以将运行统计报告及日志等打印输出，选择**“文件->打印预览”**可以做打印预览。

第四章 统计

Viacontrol 会生成管理人员所关心的公司员工各项应用程序、上网浏览和网络流量的统计报告以及统计图表，以供对员工的工作情况进行评估。

4.1 应用程序统计

应用程序统计提供了强大的统计功能，针对计算机每天的工作情况和应用程序使用的情况进行人性化统计和分析，为管理者评估员工工作效率提供了可靠的依据，并且提供了导出统计列表的功能。

选择菜单“**统计->应用程序**”可查询在某一段时间计算机(组)或用户(组)的应用程序使用情况，系统默认统计当天的应用程序使用情况。应用程序统计界面分 4 块：计算机(用户)树栏、数据显示栏、统计图、查询栏。

功能按钮说明

图标按钮	说明
	模式按钮，管理员可以选择应用程序统计的模式；
	展开按钮，如果应用程序类别有子类，可展开子类；对分项统计，可展开组内计算机或用户。对应用程序明细统计无效，图标变为灰色；
	显示 top 项，定义显示统计列表内容的条数，包括全部、前 10 条、前 20 条、自定义。当按应用程序类别统计设置展开列时，显示 top 项图标为灰色。

在统计中，开机时间和工作时间是系统默认的统计项。开机时间是指客户端机器开机后的运行时间，工作时间是指客户端机器的键盘和鼠标的操作时间。

应用程序统计可分 4 种模式：

1. 按应用程序类别统计

在应用程序分类中，管理员可对客户端机器所使用过的所有应用程序进行分门别类，以方便对应用程序类别进行统计。通过统计结果可以知道员工每日的工作情况，各个部门每日的工作情况等。

单击功能按钮区的模式按钮，选择“**模式->按类别合计**”，默认会统计所有的应用程序类别，统计结果分 3 列显示：

字段名称	说明
类别	应用程序分类中自定义的分类；
时间	客户端机器使用该分类中的应用程序的时间合计，系统默认按使用时间从长到短排列显示；
百分比	该分类中的应用程序使用时间占整个工作时间的百分比，默认是按照从大到小的顺序显示。

2. 按应用程序名称统计

假如需要统计具体使用过的应用程序百分比，则可以选择“**模式->按名称统计**”，这种统计模式会列出所选计算机(组)使用过的应用程序的使用的时间总和以及所占工作时间的百分比。按应用程序名称统计实际上是按应用程序的进程进行统计，统计出的结果一目了然，清楚的显示出用户大部分的工作时间是使用哪些应用程序，从而知道用户的工作效率。

3. 按应用程序明细统计

按应用程序明细统计与按名称统计类似，不是按进程，而是按该应用程序的描述进行统计。比如用户使用了 2 个不同版本的 QQ 程序，进程却都是 qq.exe，则按明细统计，会分别统计这 2 个不同版本的 QQ，而按名称统计，会把这 2 个版本的使用时间一起统计为 qq.exe。

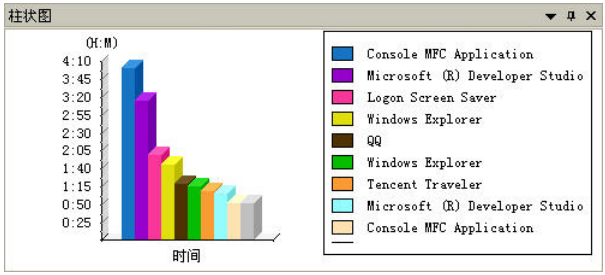
4. 分项统计

分项统计是针对计算机或计算机组分别统计不同的应用程序类别的使用百分比，默认是统计开机时间和工作时间，需要在查询栏的【类别】中增加应用程序类别进行统计。

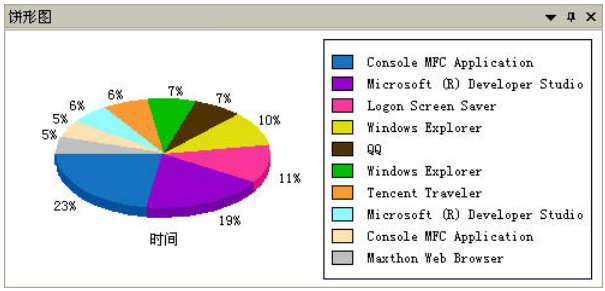
比如需要统计一个计算机组内所有计算机使用 IM、浏览器等分类的使用情况，先选中这个分组，选择统计模式为分项统计，在右边的查询栏中增加应用程序类别：IM、浏览器等预先定义好的应用程序类别，单击【查询】得到统计结果。如该组下还有子组，单击【展开】按钮，查看子组下所有计算机的统计结果。

除了生成统计报表，控制台也会生成统计图表：

柱状图：



饼状图：



4.2 上网浏览统计

很多员工会在上班时间浏览工作以外的网站，通过上网浏览统计功能可以查到用户浏览网站的情况，从而及时的发现问题并采取应对措施。

功能按钮说明

图标按钮	说明
	模式按钮，管理员可以选择网站统计的模式。
	展开按钮，对网站明细无效，图标为灰色；如果网站类别包含有子类，可展开子类；对分项统计，可展开组内计算机或用户。
	显示 top 项，定义显示统计列表内容的条数，包括全部、前 10 条、前 20 条、自定义。当按网站类别设置展开列时，显示 top 项图标为灰色。

上网浏览统计可分 3 种模式：

1. 按网站类别统计

按网站类别模式进行统计的前提是，管理员应该预先在“**工具->分类管理->网站**”中添加类别及其网站识别。这种统计模式方便用户针对不同类别的网站进行宏观统计和分析。

按类别统计默认统计所有类别的上网时间，不属于任何一个网站分类的网站识别会被自动统计到“未分类”，统计列表默认按上网时间的长短进行排序，浏览网站时间长的排在前面。

2. 按网站明细统计

按网站明细统计查询到所有访问过的网站明细，如果属于一个网站类别的，会以“网站类别 – 网站”的格式显示，如果不属于任何一个网站类别，直接显示该网站，一般按域名来统计。

按明细统计时，展开列的功能无效，默认是统计全部网站，也可以单击【显示】按钮选择 Top 项。

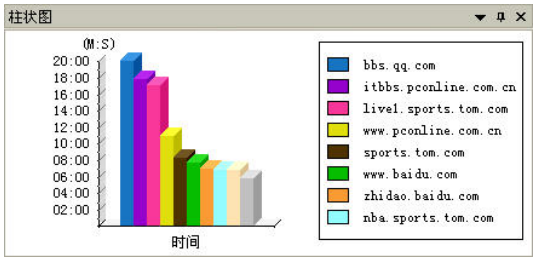
3. 分项统计

分项统计是以计算机为单位统计一个或多个网站分类的浏览时间，可以对一个计算机组或整个网络进行统计。

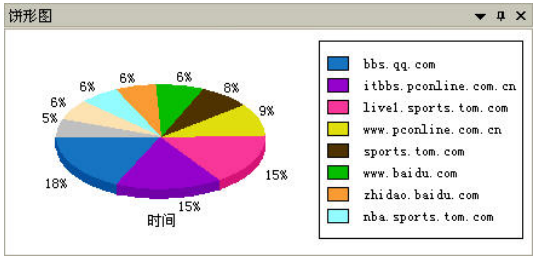
选择需要统计的计算机组，默认统计的是未分类的网站浏览时间，管理员可根据需要在右边查询栏中添加和修改网站分类。单击【展开】按钮，展开所有的子组，显示所有计算机的统计结果。

除了生成统计报表，控制台也会生成统计图表：

柱状图：



饼状图：



4.3 网络流量统计

通过查询网络流量，管理员可以快速定位网络阻塞等问题，从而做出相应的应对措施。网络流量统计包含了通讯双方的网络地址，端口，流量大小等详细信息，以帮助网络管理员查看网络使用状态并排查问题。

选择菜单“**统计->网络流量**”查看网络流量使用情况。

功能按钮说明

图标按钮	说明
	模式按钮，管理员可以选择网络流量统计的模式；
	方向按钮，包括合计、发送、接收三种流量方向；
	展开按钮，选择按计算机统计时有效，可展开组内子组的计算机 ；
	显示 top 项：定义显示统计列表内容的条数，包括全部、前 10 条、前 20 条、自定义。当按网站类别设置展开列时，显示 top 项图标为灰色。

统计条件

字段名称	说明
时间和范围	公共的查询条件
地址范围	地址范围是指通讯对方的 IP 地址，管理员可以在网络地址类别中选择地址范围进行统计，也可以直接在输入框中输入要查询的 IP 地址，如：192.168.1.1 等；
端口范围	是指通讯过程中服务方的端口，管理员可以在端口类别管理中选择端口范围进行统计，也可以直接在输入框中输入要查询的端口，输入端口需加上协议类型：TCP or UDP，如 TCP:139，如果直接输入端口号，系统默认为 TCP。

网络流量统计可分为 6 种模式：

1. 按地址明细统计

按地址明细统计是按所有 IP 地址统计端口的数据流量，从统计结果中可以看出一段时间范围内，与客户端机器通讯流量最大的对方 IP 地址，从而了解该客户端机器的网络行为。

统计结果包括网络地址及其与该 IP 地址的通讯流量。

字段名称	说明
网络地址	该列会显示所有通讯对方的 IP 地址列表，如果右侧的查询栏->地址范围中指定了一个 IP 地址范围，则只会列出指定 IP 地址范围内的 IP 地址；
全部(合计)	全部表示与该 IP 地址通讯的所有端口的流量，默认还分别统计 TCP(合计)和 UDP(合计)的流量，如果在右侧查询栏->端口范围中指定一个或多个端口类别，则会统计指定端口类别的流量；括号中的“合计”表示流量方向，单击流量方向按钮选择流量方向：合计、发送、接收。

在实际使用中，管理员可根据管理要求设置合适的地址和端口的统计范围，得到需要的网络流量统计图表。

2. 按端口明细统计

按端口明细统计是按照指定的端口范围统计对方 IP 地址范围的流量数据，从统计结果中可以看出客户端机器在哪些端口上的数据流量比较大，如果发现不正当的一些端口流量很大，可以即时采取措施关闭一些非法端口。

统计结果包括端口明细及在该端口的所有流量。

字段名称	说明
网络协议	该列会显示指定的端口范围以及协议类型，统计这些端口的数据流量；
全部(合计)	全部表示所有的 IP 地址范围在这个端口上的流量，系统默认还统计企业网(合计)和互联网(合计)的流量，合计表示流量方向，可以单击流量方向按钮选择流量方向：合计、发送、接收。

在实际使用中，管理员可根据管理要求设置合适的地址和端口的统计范围，得到需要的网络流量统计图表。

3. 按地址类别统计

按地址类别统计是按照网络地址的分类统计指定网络端口的流量，系统默认统计通讯协议在 TCP 和 UDP 下，通讯地址分别为企业网和互联网的网络流量。管理员可以在右侧的查询栏的地址范围和端口范围中选择其它的类别进行统计。

通过这种统计模式，管理员可以从宏观上分析和比较该计算机(组)在不同网络地址范围内的流量。

4. 按端口类别统计

按端口类别统计是按照网络端口的分类统计指定网络地址的流量，系统默认统计通讯地址在企业网和互联网中，通讯协议分别为 TCP 和 UDP 的网络流量，管理员可以在右侧的查询栏中的地址范围和端口范围选择其它的类别进行统计。

通过这种统计模式，管理员可以从宏观上分析和比较该计算机(组)在不同网络端口范围内的流量。

5. 按计算机和地址类别统计

按计算机和地址类别统计是以计算机或计算机组为单位统计其在指定网络地址范围内的流量。通过这种统计模式，管理员可以快速分析和比较计算机(组)之间在指定地址范围的流量不同。

如果是统计计算机组，可单击【展开】按钮展开计算机组内所有计算机，对比组内计算机在指定地址范围内的流量。

管理员可以在右侧的查询栏中更改查询范围以及地址范围，查询到有用的流量统计结果。

6. 按计算机和端口类别统计

按计算机和端口类别是指按计算机或计算机组统计指定端口范围内的流量，通过这种统计模式，管理员可以快速分析和对比计算机(组)之间在指定端口的流量不同。

如果是统计计算机组，单击【展开】按钮可以展开计算机组内所有的计算机，对比组内计算机在指定端口的流量。

注意 网络流量统计只能根据计算机来统计，不支持对用户进行统计。

第五章 日志

Viacontrol 会记录客户端机器的各种操作日志，包括：用户登录、注销日志，应用程序日志，网站浏览日志，文档操作日志，共享文档日志，文档打印日志，移动存储操作日志，资产变更日志等。通过这些具体的日志，可以查看用户在其机器上的几乎所有操作。

在所有的日志视图中，都可以做以下几种操作：

操作	说明
打印/打印预览	每个日志视图都可以打印保存、打印预览。
导出日志	根据需要导出各种日志。
删除日志	在数据视图中单击右键选择“**删除**”，管理员可根据需要选择一种删除模式：删除选中的记录、删除本页记录、删除所有满足条件的记录。
查询屏幕历史	在查看日志记录的过程中，管理员可以随时查看某条记录的屏幕历史，选择一条日志记录，单击右键“**查看屏幕历史**”会自动打开屏幕历史查看器，并且快速定位到指定日志操作当时的屏幕历史。 没有设置记录屏幕历史的客户端机器无法查询屏幕历史。

5.1 基本事件日志

选择菜单“**日志->基本事件**”查看基本事件日志，基本事件日志记录客户端系统的启动/停止，用户登录/注销，拨号，补丁管理和软件分发相关日志。

记录的日志操作类型包括以下几种：

操作类型	说明
系统启动/关闭	这里的系统是指客户端系统，因为客户端的启动/关闭和操作系统的启动/关闭对应，也可大致理解为操作系统的启动/关闭；
用户登录/注销	每一个登录到该计算机的用户的登录/注销日志；
拨号	当用户拨号连接时，客户端会记录下拨号/挂断日志
补丁管理	当管理员设置了安装补丁，客户端机器会自动安装补丁，补丁安装的所有日志会记录下来，以方便查询补丁的安装情况；
软件分发	当管理员建立了软件分发任务，会自动在目标计算机上执行，分发任务的执行日志会记录下来，以方便查询分发任务情况。

基本事件日志包含的内容有：操作类型、时间、计算机、用户、描述等信息。操作类型是记录的日志类型，如系统启动、用户登录等，描述该日志的详细信息。

基本事件日志默认显示所有的日志，管理员也可以设置各种查询条件进行有选择有目的的查询。

查询条件	说明
时间和范围	通用查询条件。
类型	类型是指基本事件日志的操作类型，默认是全部，也可在下拉框中指定一个类型进行查询，比如查询客户端机器登录过的用户以及补丁安装情况等。
描述	按照日志记录的描述信息进行查询，这是一个输入字段，支持通配符，也支持模糊查询。

5.2 应用程序日志

应用程序日志会记录客户端机器打开或关闭的应用程序，或者应用程序窗口切换信息。管理员可以通过控制台查看相关日志。选择菜单“**日志->应用程序**”，管理员可以查看所有的应用程序启动/停止和窗口/标题 切换日志。

应用程序日志类型包括：启动/停止、切换窗口、切换标题。

日志类型	说明
启动/停止	记录客户端机器上启动/停止应用程序的情况；
切换窗口	用户切换应用程序时，会记录下切换窗口的日志；
切换标题	用户在使用同一个应用程序时，也可能有多个窗口或多个标题，例如浏览器 maxthon.exe 打开多个标签页互相切换时会记录为切换标题。

注意 由于数据量较大，切换窗口和切换标题默认不记录，您可以通过“**基本策略->日志记录策略**”设置记录窗口标题变化。

应用程序日志记录包含的属性有：操作类型、时间、计算机、用户、应用程序、路径/标题等信息。

属性名称	说明
操作类型	应用程序启动/停止和窗口标题切换；
应用程序	应用程序的进程名称；
文件路径	当操作类型是启动/停止时，记录应用程序在客户端机器上的详细路径；
窗口标题	当操作类型是切换窗口/切换标题时，记录当前的应用程序的窗口标题。

系统默认显示所有的应用程序日志，管理员也可以设置各种查询条件进行有选择有目的的查询。

查询条件	说明
路径/标题	按照应用程序日志的路径或标题来查询；
应用程序	按应用程序的进程名称查询，既可以手工输入名称进行查询，也可以直接在应用程序类别中选择一个类别或一个应用程序进行查询。

按应用程序进行查询包括：手工输入应用程序名称查询、按应用程序分类查询。

1) 手工输入应用程序名称
管理员可以直接在该输入框中输入需要查询的应用程序名称，例如 qq.exe 或*game*.exe 等进行查询。

2) 通过应用程序分类
单击右边的“...”按钮打开应用程序分类窗口，左边是应用程序类别，右边是该类别中包含的所有的应用程序。
如果需要对一个类别进行查询，左边选中【应用程序类别】，在右边选择需要查询的应用程序类别，点击【确定】选择该分类进行查询；如果只需要对其中指定的一个应用程序进行查询，左边选中该程序所在的类别找到该程序，在右边选中该程序单击【确定】进行查询。

5.3 上网浏览日志

上网浏览日志会记录客户端计算机上浏览过的网站，方便管理员查看该客户端用户的网页浏览情况。选择菜单“**日志->上网浏览**”，管理员可以查看所有的上网浏览日志。

网站浏览日志支持各种常用浏览器的记录，包括：IE、TT、遨游、Firefox、Netscape 、opera 等。

网页浏览日志包含的内容有：时间、计算机、用户、标题、网址等信息。

属性名称	说明
标题	浏览的网站标题；
网址	浏览的网站的详细网址；

提示 单击右键“**打开网页**”，管理员可以快速链接到选中日志中的浏览网址，以查看该网站的详细信息。

系统默认显示所有的应用程序日志，管理员也可以设置各种查询条件进行有选择有目的的查询。

查询条件	说明
时间和范围	通用查询条件；
网址	按输入的网址查询指定网址的浏览情况，管理员可以直接输入一个网址进行查询，也可以在网站分类中指定一个类别或一个网站识别进行查询。 手工输入网址支持模糊查询。
窗口标题	根据浏览网站的窗口标题查询，如输入“娱乐”查询到所有网站标题包含娱乐的网站浏览日志。

5.4 文档操作日志

文档操作日志记录客户端机器用户对文档的操作信息，管理员通过查看日志记录可以发现用户的文档操作行为，同时为事后追查资料泄密事件提供可靠线索，增强电子文档管理的安全性。

选择菜单“**日志->文档操作日志**”查看文档操作日志，日志记录的内容包括：

属性名称	说明
操作类型	包括：创建、访问、修改、重命名、复制、移动、删除、恢复以及上传/发送
源文件	用户操作的文档名称；
路径	用户操作的文档的详细路径，当操作类型为复制、移动、重命名时，路径会记录文档的源路径和目的路径；
盘符类型	用户操作的文档所在的盘符类型，包括：硬盘、软盘、光盘、可移动盘、网络盘。 当操作类型为复制、移动时，会显示源和目的盘符类型；
应用程序	操作该文档使用的应用程序进程名称；
标题	操作该文档时的窗口标题。

在文档控制策略中和 IM 文件传送策略中可以设置文档备份策略，当客户端机器触发了这些策略，会记录备份文档日志。备份文档日志用一个别针的图标“ ”标志，比如复制的图标为“ ”。

双击备份文档日志，可以查看其详细属性，在文档名称的右侧有个按钮【副本】，点击该按钮，可以查看或保存备份文档。

系统默认显示所有的应用程序日志，管理员也可以设置各种查询条件进行有选择有目的的查询。

查询条件	说明
时间和范围	通用查询条件
操作类型	默认是全部操作类型，也可通过下拉框选择其中一种操作类型进行查询，比如，查询修改过的所有文档；
盘符类型	默认是全部盘符类型，也可通过下拉框中选择其中一种盘符类型进行查询，只查询到指定盘符类型的文档日志；
名称	按照文档名称进行查询，查询客户端机器对指定的文档有哪些操作，支持通配符和模糊查询；
大小	指定一个文件大小范围，进行查询，可查询到一定范围大小的文档操作记录；
应用程序	根据应用程序名称进行查询，可手工输入名称，也可在应用程序分类中指定一个类别或一个应用程序进行查询；
有备份文档	默认不勾选，查询到所有日志（包括有备份文档和无备份文档），勾选此复选框查询，查询到的日志都有备份文档。

5.5 共享文档操作日志

共享文档操作日志记录的是客户端机器上的共享文档被其它机器的用户操作的日志，通过查看这些日志，管理员可以知道外来计算机对本地的文档做了哪些操作。

选择菜单“**日志->共享操作**”查看共享文档操作日志记录。

共享文档日志包括的内容有：

属性名称	说明
操作类型	包括：创建、重命名、修改、删除。访问、复制和移动的操作暂不支持。
远程主机	是指访问本机共享文件的外来计算机的 IP 地址；
源文件	是指远程计算机操作的本地文档的名称；
路径	是指远程计算机操作的本地文档的详细路径。

共享文档日志可以按以下条件进行查询

查询条件	说明
时间和范围	通用查询条件；
操作类型	根据共享文档操作类型进行查询，默认是全部，也可在下拉框中选择其中一种操作类型进行查询；
名称	查询远程机器对指定的文档进行了哪些操作，输入要查询的文档名称，支持模糊查询；
远端地址或名称	按照访问本机共享的远程计算机的 IP 地址或计算机名称进行查询。

5.6 文档打印日志

文档打印日志是记录客户端机器上的打印操作，以方便日后查询。选择“**日志->文档打印**”可以查看相关打印日志。

打印日志记录包括的内容有：

属性名称	说明
打印机类型	包括：本地、共享、网络和虚拟打印机。
打印任务	打印任务记录了打印日志的核心内容，通常包含了打印的文档名称；
打印机名称	打印时所用的打印机的名称；
打印页数	打印出来的文档页数；
标题	执行打印操作时的窗口标题；
应用程序	执行打印操作的应用程序名称。

查看和保存打印记录

在打印控制策略中可以设置记录打印内容的策略，当客户端打印指定的文档时，会记录其打印内容。在打印日志中可以查看或保存打印内容。打印日志中会用一个别针的图标“ ”标志，例如共享打印机的图标为“ ”。

双击其中一条日志或右键“属性”查看其详细信息，在计算机右侧有个【副本】按钮，点击该按钮可以“**查看打印记录**”或“**保存打印记录**”。

单击【副本】按钮，选择“**查看打印记录**”打开打印内容查看器。可以放大、缩小、拖动进行查看，在有多页打印内容时，可以翻页查看，可以将图片另存为 JPG 格式保存。

单击【副本】按钮，选择“**保存打印记录**”可将打印内容保存到指定的目录。打印内容是以图片格式保存的，每页都会保存为一个 JPG 文件，如果一个打印任务有多页内容，会保存为多个图片文件。

文档打印日志可以按以下条件进行查询：

查询条件	说明
时间和范围	通用查询条件；
打印机类型	默认是全部，也可在下拉框中选择其中一种打印类型，只查询一种打印机类型的打印情况；
打印机	根据打印机的名称进行查询，方便对指定的打印机进行打印情况的统计；
计算机	是指打印机所在的计算机，假如是本地打印机，则计算机就是本机的计算机名称，如果是共享打印机，则是远程计算机即打印机所在的计算机，一般是 IP 地址；
任务名称	根据打印任务进行查询，可查询指定文档的打印情况，支持模糊查询；
页数	根据打印页数查询，方便统计滥用打印机的情况；
应用程序	根据打印时的应用程序进行查询，查询指定格式的文档的打印情况。
有打印记录	默认不选择，代表全部；如果选择该项查询，则表示查询有打印记录的打印日志。

5.7 移动存储操作日志

移动存储日志记录了客户端机器上所有移动存储设备的插入拔出情况，对其在网络内的使用情况进行全面监控和记录，提高文档保密的安全性。

选择菜单“**日志->移动存储操作**”查看所有移动存储的使用日志，内容包括：

属性名称	说明
操作类型	插上或拔出；
移动存储类型	是否为加密盘，其中，空表示非加密盘；
卷序列号	一个移动存储的唯一标志，在移动存储分类中可以查看这个卷序列号对应的移动盘；
设备描述	该移动盘的描述信息，也就是该设备的名称；
卷标	移动盘的卷标名称。

移动存储操作日志可以按以下查询条件进行查询：

查询条件	说明
移动存储	按移动存储的序列号查询，需要在移动存储分类中指定一个分类或一个移动盘进行查询，便于统计一类或一个移动盘的使用情况；
操作类型	默认是全部，也可在下拉列表中选择插上或拔出进行查询，可以快速查询客户端机器所有插入过的移动盘日志。
移动存储类型	按是否加密盘来查询，默认为全部，可以在下拉列表中选择加密盘或非加密盘进行查询。

5.8 资产变更日志

资产变更日志记录的是客户端机器上硬件和软件的变化情况，以帮助管理员维护和管理企业内的资产信息。

选择“**日志->资产变更**”查看所有软硬件的变化日志，包括：

属性名称	说明
操作类型	资产的增加、删除、变化；
类型	属于硬件变更还是软件变更；
描述	对发生变化的资产的描述信息。

资产变更日志可以按以下条件进行查询：

查询条件	说明
类型	按照资产类型查询，查询到所有的硬件变更或软件变更，方便管理员分别查看这 2 种资产的变化情况；
操作类型	变更的方式，管理员可查询到增加的资产、删除的资产以及变化的资产；
描述	根据资产的描述信息进行查询，查询资产的变更情况。

5.9 策略日志

策略日志会记录所有客户端机器触发的策略日志，以方便日后查询员工的操作行为。

选择“**日志->策略日志**”可查看到策略日志，包括：

属性名称	说明
报警级别	报警级别有 3 种：低、重要、严重，管理员在设置策略的时候可以选择报警的级别；
涉及策略	客户端机器的操作触发的策略类型；
描述	客户端机器的操作行为以及触发的策略描述。

策略日志可以按以下条件进行查询：

字段名称	说明
最低级别	默认是全部，查询到所有报警级别的日志，如果选择低，则查询低、重要、严重的日志；选择重要，只查询重要和严重的日志；
策略类型	默认是全部，也可指定其中一种策略类型进行查询，只查询该策略的日志；
内容	根据描述内容进行查询，支持模糊查询。

5.10系统日志

选择菜单“**日志->系统事件**”，管理员可以查看服务器的启动和停止日志，非法计算机接入网络的报告以及服务器和客户端之间的通讯错误日志。

注意 客户端连不上服务器或通讯不正常时，可查看系统日志，以便发现错误原因。

第六章 策略

6.1 策略简介

管理员可以通过策略限制客户端对计算机和网络的使用，有效规范员工的电脑使用，提高生产效率。

策略通用属性说明

策略的设置包含很多属性，在各种类型的策略属性中，有一些属性是通用的，含义也相同。

策略属性	说明
名称	只是用户自己定义的一种对该条策略的描述。与策略的执行功能无关。当添加一条策略时，控制台会默认添加名称，管理员也可以自定义名称。
时间	指定策略生效的时间范围。系统默认是全天，可以是已定义的时间类型(在“**工具->分类管理->时间类型**”中设置)； 如果没有符合要求的时间类型，可以选择“**自定义**”，在弹出的时间选择框中直接设置时间范围。
模式	是指满足了策略条件后执行的模式，包括禁止、允许、忽略和不操作。详情请参考后面的模式说明。
动作	策略执行的同时产生的动作，包括报警，警告，锁定计算机三种类型。这 3 种动作可以同时设置，也可以设置其中的一种。详情请参考后面的动作说明。
到期时间	指定策略生效的终止时间。默认策略是<始终有效>。如需要设置到期时间，在设置窗口中选中“**启用**”并设置到期时间。不允许设置小于当前系统时间的到期时间。如果此策略已经过期，则此条策略的字体将会以深灰色显示，【到期时间】中的时间值显示成红色。
仅离线生效	当客户端和服务器无法通讯时，则客户端视为处于离线状态。选中“仅离线生效”表示该策略仅当客户端处于离线状态时才生效，主要是计算机使用者出差，回家或网线故障的情况。如果不选中此项，表示该策略始终生效。

策略有 4 种模式：允许、禁止、忽略、不操作。

模式	说明
允许	允许进行某种操作。如果某个操作匹配的策略模式为允许，则允许，并不再继续判断其下面的策略。
禁止	禁止进行某种操作。如果某个操作匹配的策略模式为禁止，则禁止，并不再继续判断其下面的策略。
忽略	对操作既不允许，也不禁止。如果某个操作匹配的策略模式为忽略，会执行本策略所设置的动作，然后继续匹配下面的策略，决定该操作是允许还是禁止。
不操作	既不允许，也不禁止（主要用于基本策略和设备策略中）。如果某个项目或者设备匹配的策略模式为不操作，则不做允许或者禁止，并不再继续判断其下面的策略。

当客户端机器触发了策略，可以产生相应的动作，动作包括：报警、警告、锁定计算机。

动作	说明
报警	当此策略匹配后，客户端会向服务器发送报警信息，在控制台上会弹出报警以提示管理员，同时此报警日志也会作为策略日志记录下来。 可以通过菜单“**工具->选项->实时报警->气泡设置**”选择当前控制台是否弹出报警气泡，通过“**工具->警报**”查看实时报警信息。 报警可以设置为三种级别：低、重要和严重。
警告	当此策略匹配后，在客户端会弹出对话框，警告客户端的使用者执行了某些限制的操作。管理员可以在警告信息中自定义消息框显示的内容。
锁定计算机	当此策略匹配后，客户端计算机会被自动锁定，使用者将不能进行任何操作。 在控制台的“**控制->解锁**”可以对客户端进行解锁。

策略的匹配优先级

策略采用类似于防火墙的策略方式，每组策略可由多条策略组合而成，按照先后关系进行匹配，按最先匹配的策略执行规则；同时每个对象还会自动继承父对象的策略。

管理员可以依次设置整个网络策略、组策略、计算机策略和用户策略；策略匹配的优先级由高到低依次为：用户策略 > 用户组策略 > 计算机策略 > 计算机组策略。

从父组继承的策略都会用浅绿色背景显示，且不能修改父组策略。策略涉及到字符串的输入字段都支持通配符，支持输入多个，中间以半角分号“;”或半角逗号“,”隔开，其中每个字符串最多包含 3 个通配符。

策略的图标按钮说明

图标按钮	说明
	新建，点击该按钮新增加一条策略；
	上移，将选中的策略上移一个位置；
	下移，将选中的策略下移一个位置；
	删除，点击该按钮删除选中的策略；
	恢复，取消新建或修改策略时点击该按钮；
	保存，设置或修改策略后需保存才会生效。
	表示该策略的模式是“允许”；
	表示该策略的模式是“禁止”；
	表示该策略的模式是“忽略”；
	表示该策略的模式是“不操作”；
	表示该策略设置了报警；
	表示该策略设置了警告；
	表示该策略设置了锁定计算机；
	表示该策略设置了到期时间。

6.2 基本策略

通过基本策略可以规范网络内计算机的操作权限，限制客户端机器对计算机系统设置的任意修改，防止恶意或无意的破坏，增强计算机的使用安全性。

基本策略主要是通过修改注册表值来实现的。基本策略和设备控制策略与其他的策略不同，是一种状态维持的策略，而不是实时的触发策略；因此对策略的修改，删除等处理和其他的策略不同。

基本策略支持的项目包括：控制面板，计算机管理，系统，网络，IP/MAC 绑定，ActiveX 控件。

控制面板包括以下 5 项：

基本策略项	说明
控制面板	包括控制面板上的各个功能；
设置屏幕属性	限制客户端设置桌面，屏幕保护程序以及桌面外观等；
添加打印机	限制客户端添加打印机；
删除打印机	限制客户端删除打印机；
快速切换用户	禁止在 Windows 系统里通过切换用户的方式同时登录多个用户（仅 XP 系统有效）。

计算机管理包括以下 5 项：

基本策略项	说明
设备管理器	限制客户端机器使用设备管理器；
磁盘管理	限制客户端机器使用磁盘管理；
本地用户和组	限制客户端机器使用本地用户和组的控制面板管理项；
系统服务管理	限制客户端机器使用系统服务管理；
其它计算机管理	限制客户端使用计算机管理中除了上面四项以外的其它管理功能，包括：事件查看器、共享文件夹、性能日志和警报等。

系统包括以下 5 项：

基本策略项	说明
任务管理器	限制客户端使用任务管理器；
注册表编辑器	限制客户端使用注册表；
命令提示符	限制客户端使用命令提示符，9x 系统下是 command 程序，NT 及以后版本操作系统下是 cmd 程序；
运行注册表中 Run 下的程序	如果模式为禁止，Run 下的程序会在系统开机的时候不会启动，需注销或重启计算机生效；
运行注册表中 RunOnce 下的程序	RunOnce 是指在开机的时候启动一次，下次开机就不会运行了，如果模式为禁止，则 RunOnce 下的程序不会启动，需注销或重启计算机生效。

网络包括以下 6 项：

基本策略项	说明
修改网络属性	限制客户端修改网络属性；
显示“网络邻居”	模式为禁止时，桌面上的网上邻居会隐藏，需要注销或重启生效；
修改 Internet 选项	限制客户端修改 Internet 选项设置；
默认网络共享	如果模式为禁止，客户端上的默认共享被禁止；
使用网络共享	如果模式为禁止，客户端不能共享本机文档；
增加网络共享	如果模式为禁止，客户端新增的网络共享会被禁止。

IP/MAC 绑定

基本策略项	说明
修改网络 IP/MAC 配置	限制客户端修改网络属性； 为了禁止用户随意修改 IP，可使用该功能禁止修改网络 IP/MAC 配置。设置策略后，客户端会保存当前的 IP 和 MAC 信息，一旦发现用户有修改，立即会改回保存的 IP/MAC。 如果用户需要修改 IP，需要先去掉该策略。

ActiveX 控件包括以下 4 种控件：

基本策略项	说明
聊天类 ActiveX 控件	限制客户端使用聊天类 ActiveX 控件，用户使用聊天控件时会被禁止；
影音类 ActiveX 控件	限制客户端使用影音类 ActiveX 控件，一般在互联网上听歌或看视频文件会用到该类控件，禁止该项，用户无法听歌或播放视频；
游戏类 ActiveX 控件	互联网上的一些小游戏可能需要安装游戏类控件，禁止该项，此类小游戏无法正常运行；
FLASH 类 ActiveX 控件	播放 FLASH 文件会用到该类控件，禁止该项，FLASH 文件无法正常播放。

其它

基本策略项	说明
系统还原	为了防止客户端机器通过系统还原来卸载客户端，可以禁止该项，则系统还原功能被禁止。

策略示例

假如您的需求是：在公司时禁止修改 IP 地址，但是允许回家或出差的时候修改 IP。管理员可以对目标计算机（如整个网络）设置基本策略：

① 先设置一条策略，禁止修改 IP/MAC 属性；
② 再设置一条离线策略，允许 修改 IP/MAC 属性 仅离线生效。

按照策略匹配原则，后设置的策略在上面，因此策略②优先于策略①，当离线状态时，策略匹配，允许修改 IP/MAC；当在线状态时，与策略②不匹配，接着向下匹配策略①，条件满足，执行策略禁止修改 IP/MAC 属性。

注意 基本策略的修改网络 IP/Mac 配置，系统还原，网络共享对计算机有效，对用户是无效的。

6.3 设备控制策略

设备控制策略主要是对与计算机有关的各种设备进行控制，规范企业内计算机对存储设备、通讯设备各种类型的设备使用，防止企业机密资料通过这些计算机外部设备泄露出去，增强企业管理的规范性和安全性。

设备控制策略支持的设备列表包括：存储设备、通讯接口设备、拨号、USB 设备、网络设备、其它设备。

存储设备包括：

设备类型	说明
软盘	软盘控制器，禁止该项，则软驱也被禁止；
光盘	DVD/CD-ROM 驱动器；
刻录/烧录机	对刻录/烧录的行为进行控制，可以读盘；
磁带	对磁带做控制；
可移动设备	除硬盘（ide、scsi、sata 接口）外的存储设备，包括 U 盘，移动硬盘，记忆棒，智能卡，MO，Zip。

通讯接口设备包括：

设备类型	说明
串口	COM 端口；
并口	LPT 端口；
USB 控制器和连接器	通用串行总线控制器和连接器（HUB）；
SCSI 接口	scsi 和 raid 控制器，scsi 硬盘会用到该接口；
1394 控制器	IEEE 1394 总线主控制器，1394 接口，通俗的说就是 1394 插槽，同 USB 控制；
红外线	红外线设备；
PCMICA 卡	一个 PCMCIA 接口，通俗的说就是 PCMCIA 插槽，同 USB 控制器；
蓝牙设备	蓝牙设备；
MODEM	拨号设备；
直接电缆连接	用 usb 线、com 口对连线或并口对连线直接把两台计算机连接起来的行为。

拨号包括：

设备类型	说明
拨号连接	对拨号连接做控制。

USB 设备包括：

设备类型	说明
USB 键盘	控制 USB 键盘的使用；
USB 鼠标	控制 USB 鼠标的使用；
USB Modem	控制 USB Modem 的使用；
USB 映像设备	控制 USB 接口的摄像头、扫描仪、数码相机；
USB CDROM	控制 USB 接口的 CDROM；
USB 存储	控制 USB 接口的存储设备；
USB 硬盘	控制 USB 硬盘的使用；
USB 网卡	控制 USB 网卡的使用；
USB 其他设备	控制非以上 USB 接口的其它设备。

网络设备包括：

设备类型	说明
无线网卡	控制无线网卡的使用；
PnP 网卡(USB，PCMICA)	可热插拔的网卡；
虚拟网卡	非物理连接主板或非主板自带的网卡。

其它设备包括：

设备类型	说明
声音设备	声音、视频和游戏控制器；
虚拟光驱	控制虚拟光驱的使用；
任何新设备	任何一个插入计算机的新设备，如果模式为禁止，所有的新插入的设备都被禁用。

策略示例 1

在一些企业，上班时间不允许听歌、视频等行为，此时可以设置设备控制策略禁止声音设备。

策略：时间范围选择工作时间”，模式选择禁止，在设备列表中勾选“声音设备”，则设置了该策略的计算机的声卡被禁用。

策略示例 2

为了保护企业内部的重要文档资料，需要限制员工通过可移动设备或刻录机等设备将内部资料拷走，可设置策略禁止这些设备。

策略：模式选择“禁止”，在设备列表中勾选需要禁止的设备，如：可移动设备、软盘、光盘、刻录机等，则设置了策略的计算机无法使用这些设备。

6.4 应用程序策略

在企业中，可能有些应用软件是管理者不希望员工使用的，例如一些 BT、迅雷下载工具，聊天工具以及游戏类的软件。应用程序控制策略可以限制客户端机器对这些应用程序的使用。

新添加的策略，应用程序默认是全部，需要管理员来指定应用程序，应用程序的控制有 2 种方式：

1. 通过进程名称来禁止

管理员直接添加应用程序的名称，如 thunder.exe，此时策略是通过字符串匹配的，如果客户端修改了应用程序名称改为 thunder123.exe，则策略就无法生效；要避免这种情况可以采用第二种方法去控制；

2. 通过应用程序分类来禁止

管理员选择应用程序分类中的一个分类（可以将要禁止的应用程序都放到这个分类中），即使客户端修改了应用程序名称，只要程序本身没有变化，策略依然生效。

警告 禁止全部应用程序会导致大部分进程被禁用，为避免可能的损失，请设置策略时谨慎操作。

6.5 上网浏览策略

上网浏览策略可以有效控制员工访问网页的行为，禁止访问与工作无关的网站或者恶意网站，提高工作效率，保护内网安全。

管理员可以直接添加网站，也可以在网站分类中指定一个网站类别进行控制，对网站分类的设置在“**工具->分类管理->网站分类**”中添加或修改。

网站名称可以是完整的网址，也可以包含通配符，如：“*.baidu.com”，“*mail*”，“*game*”，“*.com/mail/*”等。

策略示例

为了防止员工访问非法的网站，可以设置上网浏览策略禁止访问这些网站或者只允许访问指定的一些网站。假如您的需求是只允许访问指定的网站，可以设置一组策略：

① 先设置一条策略，禁止 <全部> 网站；
② 再设置一条策略，允许 指定网站（将允许的网站都添加进去）。

这样，指定的网站可以访问，而其他所有的网站都无法访问了。

6.6 屏幕记录策略

屏幕历史可以记录客户端机器的所有操作行为，因为数据量较大，系统默认是不记录的，管理员可根据实际需要来设置策略记录屏幕记录。

策略的属性包括：

策略属性名称	说明
应用程序	设置需要记录的应用程序，默认是<全部>，可以指定管理员关心的应用程序进行记录；
时间间隔	设置记录屏幕快照的时间间隔，默认是 15s，也就是说每隔 15s 截一次屏幕。时间间隔的有效范围是 1-999，只有在【记录】模式下有效。

通过针对不同的应用程序，设定不同的记录频率，可以对一些用户关注的应用做频繁的记录，而对不重要的程序则不记录或少记录。

注意 屏幕记录的时间间隔越小，产生的数据量越大，管理员需要根据实际需要适当的调节屏幕记录的时间间隔。

6.7 日志记录策略

客户端的所有日志默认都是记录的，除了窗口标题日志。企业内可能会有一些需求，并不是所有的日志都希望记录下来，比如拨号日志、即时通讯日志等，此时可通过日志记录策略来控制日志的记录类型。

系统有一条默认策略，除了窗口标题变化日志不记录，其它所有日志都默认记录。

假如您需要不记录一些日志，可以添加一条策略，设置为不记录，勾选不需记录的日志项，保存策略即可。

日志记录项	说明
系统启动/关闭	基本事件日志中的系统启动或关闭日志；
用户登录/注销	基本事件日志中的用户登录或注销日志；
拨号	基本事件日志中的拨号日志；
策略控制	策略报警日志；
硬件变更	资产变更日志中的硬件变化日志；
软件变更	资产变更日志中的软件变化日志；

日志记录项	说明
应用程序	应用程序日志可以针对指定的应用程序设置为记录或不记录，也可针对有可视窗口的应用程序进行设置。
仅可见窗口	是指有前台窗口的应用程序。
应用程序	管理员可以手工指定应用程序，也可以在应用程序分类中选择类别，支持通配符。
窗口标题变化	窗口标题变化默认是不记录的，可以添加策略设置记录该项，并可以对指定的应用程序进行记录。
应用程序	管理员指定窗口标题变化的应用程序名称，可手工输入，也可在应用程序分类中选择类别，支持通配符。
网页浏览	管理员可以设置不记录网页浏览日志，并且针对指定的网站记录或不记录。
网站	手工输入网站地址，支持通配符，也可以预先在网站分类中分好类别，选择网站类别。

日志记录项	说明
文档操作	文档操作日志，管理员可以设置不记录某些文档日志，确保记录下来的日志是有用的。
盘符类型	包括：硬盘、软盘、光盘、可移动盘、网络盘和未知盘符。比如可以设置不记录硬盘上的文档日志。
文件名称	设置需要记录或不记录的文件名称，支持通配符，比如设置不记录*.txt；*.log 等。
应用程序	指定文档操作的应用程序。
打印操作	客户端的文档打印日志
打印机类型	选择需要记录或不记录的打印机类型。
应用程序	设置打印文档时的应用程序。
共享文档	共享文档操作日志
文件名称	共享操作的文档名称，支持通配符。
网络地址范围	远程访问该客户端共享文档的计算机 IP 地址范围，管理员可以针对性的设置不记录部分机器的访问记录。

日志记录项	说明
邮件	邮件内容，对于不想记录下来的邮件类型，可以设置不记录某些邮件。
发送/接收	选择邮件的方向，发送或接收。
发件人	设置邮件的发件人的地址，支持通配符，则发件人符合的邮件会根据策略去记录或不记录。
收件人	设置邮件的收件人的地址，支持通配符。
邮件大小（>=KB）	邮件大小>=该值的邮件被记录或不记录
不记录附件	只有在策略模式为“记录”时有效，如果勾选该项，则邮件的附件不会被记录，在控制台上显示是带有附件的，只是无法查看和保存其内容。
即时通讯	即时通讯内容，管理员可以根据需要设置记录其中的一些聊天工具的内容。
应用程序统计	应用程序统计数据。
网页浏览统计	网页浏览统计数据。
网络流量统计	网络流量统计数据。

6.8 远程控制策略

通过设置远程控制策略，可以控制客户端机器能否被远程控制或者被远程控制的方式。

远程控制类型有远程控制和远程文件传送两种。

只有选择了上面两项中的至少一项后，才能设置下面其它属性：

策略属性名称	说明
需要强制确认	此项只有在策略模式为【允许】时有效。勾选此项，表示只能通过用户授权的方式进行远程控制；不勾选此项，表示可以通过用户授权和密码授权这 2 种方式进行远程控制。 关于这 2 种授权方式可参照后面的“**维护->远程控制**”。
管理员名称	对登录当前控制台的管理员用户进行控制。比如：可以限制某些管理员用户对指定客户端机器的远程控制方式，需要强制确认。管理员账户在“**工具->账户**”中设置。
控制台 IP 地址	对当前控制台所在计算机的 IP 地址范围进行控制。比如： 限制一个 IP 范围内的所有计算机通过登录 Viacontrol 控制台使用远程控制功能。 如果输入是 0.0.0.1-255.255.255.255，或什么也不输入，或不是有效 IP 地址段，会认为是所有的 IP 地址，用<全部>表示。
控制台名称	对登录控制台的计算机名称进行控制。

管理员名称、控制台 IP 地址和控制台名称支持分号“;”或逗号“,”作分隔符，可同时设置多个。

6.9 系统报警策略

系统报警功能是针对计算机的软硬件变化以及系统的关键设置变化给出实时报警，方便管理员及时发现网络内计算机的变化，并做出应对措施，增加局域网内计算机的可维护性。

系统报警策略支持的报警项包括：

系统报警项	说明
硬件变化	硬件资产中任意一个资产的变化都会报警，方便管理员对网络内计算机硬件资产的维护；
插入设备	插入计算机外部设备的报警，会记录该设备的名称；
拔出设备	拔出计算机外部设备的报警，与插入对应；
插入存储设备	对存储设备的使用情况报警，会记录存储设备的名称，提醒管理员，防止使用非法外来存储设备；
拔出存储设备	跟插入存储设备报警对应；
插入通讯设备	对计算机通讯设备的使用报警，会记录通讯设备的名称，以提醒管理员，防止使用非法外来通讯设备；
拔出通讯设备	跟插入通讯设备报警对应；

系统报警项	说明
软件变化	软件资产的增加、删除、变化，方便管理员对网络内计算机软件资产的维护；
系统服务变化	客户端机器的系统服务的增加和删除报警，帮助管理员查找病毒或系统问题；
启动项变化	客户端机器的系统启动项的增加、删除和变更报警，协助管理员查找病毒或系统问题；
系统时钟改变	客户端机器的系统时钟的变化；
计算机名称变化	客户端的计算机名称更改报警，提醒管理员，阻止客户端的非法操作；
网络配置变化	客户端机器的网络属性的变化，帮助管理员发现网络问题。

系统报警的内容包括报警类型以及具体的描述信息，帮助管理员快速定位问题发生的位置并很好的解决问题。

6.10流量控制策略

流量控制策略是针对客户端机器的网络流量进行合理控制，避免部分机器任意的使用网络资源造成网络堵塞，影响整个企业内的正常工作，同时也可以限制指定端口的流量，禁止员工的任意下载行为。

网络流量策略只对计算机有效，对用户无效。策略属性包括：

策略属性名称	说明
网络地址范围	设置通讯对方的 IP 地址范围。默认地址范围是{全部}，可以手工逐个添加，也可以在网络地址分类中指定类别，指定的类别用{...}表示；
端口范围	设置通讯中用到的端口范围。默认端口范围是{全部}，包括：TCP：0-65535；UDP：0-65535；ICMP。可以手工添加端口或端口范围，也可以在端口分类中指定端口类别，用{...}表示。 输入自定义端口时要在前面加上“TCP：”或“UDP：”来区分 TCP 端口和 UDP 端口，如果不加，则认为是 TCP 端口。
流量方向	通讯过程中的网络流量方向，由客户端机器到对方计算机的流量为发送流量，反之为接收流量。发送流量+接收流量=合计流量；
限制速度	设置流量的限制大小，单位是 KB/s，模式为不限流量时不可用。

如果策略模式为限制流量，则当客户端在指定 IP 范围，指定端口范围和指定的方向的流量超过设置的限制速度时，客户端便会暂停下载/上传，直到平均流量低于指定值，从而达到限制流量的目的。

如果策略模式为忽略，但没有设置任何动作，则限制速度的属性无效，如果设置了动作（报警，警告，锁定计算机），当客户端在指定 IP 范围，指定端口范围和指定的方向的流量超过设置的限制速度时，便会触发所设的动作，但是不会限制该流量。

策略示例 1

为了限制客户端机器任意访问互联网，严重占用企业带宽，从而给整个企业的网络访问带来影响，可以设置流量控制策略来控制指定机器的流量。

策略：模式选择“限制流量”，指定地址范围，如：互联网，端口范围可以为默认，也可以指定端口，选择流量方向并设置限制速度如 20k/s，则设置策略的客户端机器访问网站或上传/下载的速度被限制在 20k/s。

策略示例 2

通过流量控制策略，也可以禁止客户端机器与指定 IP 或指定端口之间的通讯，假如需要禁止 FTP 下载，可以设置策略：模式选择“限制流量”，IP 地址范围可以是{全部}，设置端口为 TCP:21，限制速度为 0KB/s。

6.11网络控制策略

网络控制策略可以有效控制客户端机器与其他非法计算机之间的通讯，同时阻断一些恶意端口或下载端口，防止病毒入侵，保护内网安全。

网络控制策略是针对计算机的，在用户模式下无效。策略属性包括：

策略属性名称	说明
通讯方向	有双向，出站和入站三种(是指物理上的通讯方向)。出站和入站是相对于客户端机器来说的，也就是客户端机器主动连接其他计算机，即为出站。
端口范围	与流量控制策略中的端口范围含义相同。
网络地址范围	与流量控制策略中的网络地址范围含义相同。
对方是客户端	判断通讯对方机器是不是客户端计算机，只有勾选了该项，下面的属性才有效。如果不勾选，则表示不判断对方是否客户端。
属于相同分组	对于属于相同分组的客户端机器之间的通讯做控制，这里的相同分组是指当前设置策略的客户端机器所在的分组，不包含子组，也不包含上一层的分组；
属于指定分组	对于指定分组的计算机之间的通讯做控制，分组的指定在下面“所属分组”中设置，只有勾选了该项，“所属分组”才有效；
所属分组	指定通讯对方计算机所属的分组，只有指定了分组，才能选择“包含子组”；
包含子组	选择是否包含指定分组中的子组。

策略示例 1

为了保护内网安全，企业需要禁止一些恶意端口或下载端口，可以通过网络控制策略来实现。

策略：选择模式为“禁止”，设置需要阻断的地址范围，设置需要禁止的端口，如：80 端口，21 端口等。如果设置了 80 端口，则客户端机器无法访问网页，如果设置了 21 端口，则客户端机器无法使用 FTP 下载。

策略示例 2

在整个企业中，有些部门的计算机可能是非常重要的，是不允许部门之外的计算机访问的，通过网络控制策略也能很好的解决这个问题。

对整个部门设置策略:

① 先设置一条策略，禁止 网络地址范围：局域网
② 再设置一条策略，允许 对方是客户端+属于相同分组

这样该部门内的计算机只能和本部门的计算机通讯，设置策略之前，管理员需要将所有该部门的计算机放在同一个分组。如果该部门还有其他没有安装客户端的计算机，请把 IP 地址范围添加到允许的策略中。

策略示例 3

在实际运用中，网络控制策略也可以和接入检测策略结合起来使用，防止外来的计算机和内部的计算机通讯。

对于网内安装了客户端的计算机，可以设置网络控制策略，只允许与企业内的计算机通讯，这样外来的计算机就无法访问设置了该策略的客户端机器。

对于网内没有安装客户端的计算机，管理员可以在接入检测中，设置这部分机器为“保护”，并启动接入控制功能，这样外来的计算机将被视为“非法”的计算机，不能与这部分“保护”的计算机通讯。

6.12邮件控制策略

邮件控制策略是为了防止企业内部重要资料通过邮件的方式泄露出去，在不影响员工正常使用邮件的前提下规范邮件的发送内容,保障企业的内部资料安全。

邮件控制策略只能对发送邮件进行控制，对接收邮件无法控制。暂时不支持网页邮件和 Lotus 邮件的发送控制。邮件控制策略是针对计算机的，在用户模式下无效。策略属性包括：

策略属性名称	说明
发件人	对发件人的邮箱地址做控制，支持通配符，支持输入多个，以“,”“;”作为分隔符；
收件人	对收件人的邮箱地址做控制，收件人也包括抄送人和密送人的邮件地址，输入规则同“发件人”；
主题	对发送邮件的主题名称进行控制，输入规则同“发件人”；
包含附件	对发送的邮件是否包含附件做控制。勾选此项，只对包含附件的邮件做控制；不勾选此项，对所有满足条件的邮件做控制(包含附件和不包含附件)；
附件名称	如果勾选了“包含附件”，可以在这里输入附件名称，对指定附件名称进行控制，输入规则同“发件人”；
邮件大小(>=KB)	对发送的邮件大小进行控制，默认是 0，也就是全部，输入要控制的邮件大小，则>=输入值的邮件受控制

策略示例 1

为了防止企业内计算机通过邮件的方式将内部机密资料发送出去，一般需要对发送的附件进行控制，附件名称包含指定关键字的邮件将被禁止发送出去。

设置策略：禁止 包含附件 附件名称：如 *关键字*，则客户端机器上发送的邮件中，包含了附件，且附件名称中包含了“关键字”的邮件被禁止发送。

策略示例 2

一些企业可能需要限制邮件的发件人，只允许员工使用指定的内部邮箱发送邮件，使用其它邮箱发送邮件被禁止，规范管理员工使用电子邮件，也方便对外发的邮件进行严格把关。

设置策略:
① 先设一条策略：禁止 全部邮件;
② 再设一条策略：允许 发件人：指定发件人，如：*@teclink.com.hk。

这样只有发件人的邮箱地址包含@teclink.com.hk 的邮件才能发送成功。

6.13IM 文件传送策略

IM 文件传送策略可以有效控制企业内计算机通过即时通讯工具将企业内部资料传送出去，从而保障了内部资料的安全性。

IM 文件传送策略支持各种即时通讯工具，包括：QQ、MSN、SKYPE、TM、UC、RTX、雅虎通、POPO、阿里旺旺、ICQ 等。策略属性包括：

策略属性名称	说明
文件名称	设置需要控制的 IM 传送的文件名称，支持通配符，支持“;”“,”作为分隔符；
限制文件大小	只有当模式为“禁止”时，此属性有效。意为：禁止传送大于此值的文件。此值的范围为：0 – 100000 KB；
是否备份	选择是否对指定的发送文件备份。备份的文件在“日志->文档操作”中查看或保存；
备份文件最小大小(>=KB) 备份文件最大大小(<=KB)	如果选择了备份文件，则可以限制备份文件的大小这里可以设置备份文件大小的一个范围，分别设置一个最小值和最大值。在此范围内的文档将被备份，否则不备份。

策略示例

为了保护内部资料的安全，防止员工通过即时通讯工具将文件传送出去，可以设置 IM 控制策略，禁止发送包含指定关键字的文档，并且备份其他发送出去的文档。

设置策略:

① 先设一条策略：允许　勾选备份选项;
② 再设一条策略：禁止　文件名称：*关键字*。

则客户端机器发送包含关键字的文件时会被禁止，而其它文档可以正常发送，但是会自动备份下来,管理员可以到文档操作日志中查看发送的文档是否合法。

6.14文档操作策略

文档控制策略可以有效的限制客户端访问机密文档的权限,防止机密文件外泄，同时文档备份功能也能避免重要文档因为误操作而带来的损失。

文档操作策略的属性包括：

策略属性名称	说明
操作类型	为了方便理解和控制，把文档操作类型简单的分为：读取、修改、删除这 3 种。其中，允许修改就一定可以读取，允许删除就一定可以读取和修改。
读取	即访问文档；
修改	包含了访问和删除之外的所有操作，包括创建、重命名、修改、复制、移动和恢复。只有选中了该项，“修改前备份”和“复制/移动到备份”才有效；
删除	删除文档，只有选中了该项，“删除前备份”才有效。
盘符类型	默认是全部盘符类型，至少要选择一种盘符类型，否则自动识别为全部。选中“盘符类型”，可以用 Ctrl + A 对其所有子项进行全选或全不选；
文件名称	指定需要控制的文件名称，可以包含路径，如 E:\work*，则 work 这个文件夹下的所有文件都生效。文件名称支持通配符，支持“;” “,”作为分隔符；
修改前备份	备份修改的文件，只会备份修改之前的源文件，以防止重要文件被恶意或无意修改；
复制/移动到备份	复制/移动到指定盘符类型时备份文件，方便检查客户端机器是否将重要文件复制/移动到非法的盘符；
删除前备份	备份客户端删除的文件，避免重要资料被误删除而带来的损失；
备份文件最小大小(>=KB)，备份文件最大大小(<=KB)	指定要备份的文档大小范围，与 IM 文件传送策略中含义相同；
应用程序	指定文档操作的应用程序。

策略示例 1

可能有些重要文件不允许所有用户任意修改，需要限制一部分员工的权限，只允许访问，不允许修改和删除。

设置策略：禁止 操作类型：修改和删除 指定文档名称 选择备份方式，则用户对指定的文档只有访问的权限。

策略示例 2

为了防止用户对一些文档的误操作：删除或修改，管理员可以设置策略针对这种情况备份指定的文档。

设置策略：允许 操作类型：修改和删除，指定文档名称，选择备份， 则用户对这些文档的使用不受限制，但是修改和删除时会自动备份文档，备份的文档

到文档操作日志中查看。

注意 如果文档策略中设置了备份,可能会导致备份的文档数据量很大,建议在设置策略时，尽量精确定位，避免备份大量无用的文档。

6.15打印控制策略

管理员通过设置打印机的类型及开启打印文档的应用程序，有效地限制员工打印文档，既保障机密文档不外泄，也极大地节约企业资源。

打印控制策略的属性包括：

策略属性名称	说明
打印机类型	有共享、网络、本地和虚拟打印机四种类型。 如果四种类型都不选择，则认为是所有类型的打印机，即相当于四种打印机全部选中，在保存后，这个属性中的四种类型会全部被选中。
打印机描述	设置打印机名称。可以指定网内某台计算机上的打印机，如：“\\server*”表示\\server 上的所有打印机；“SomePrinter”为名称为 SomePrinter 的打印机。
应用程序	指定进行打印的应用程序。
记录打印内容	模式为允许或忽略时可选；模式为“禁止”时不可选。 如果选择该项，策略匹配该条策略，记录或不记录打印内容；如果不选择该项，则继续匹配下一条策略，决定是否记录打印内容。
记录模式	默认不记录，如果需要记录打印内容，可在下列表中选择“记录”。
最大记录页数	记录模式为“记录”时有效，设置记录打印文档的最大页数，管理员可以根据实际情况设置该项，记录的页数越多，则占用的空间会越大。 记录的打印内容到控制台的“**日志->文档打印日志**”中查看。

策略示例

在企业中，需要限制客户端机器的打印操作，以防止资料外泄或滥用打印机的问题。

设置策略：禁止共享打印机、网络打印机 打印机描述：输入打印机名称 应用程序：指定打印的应用程序，默认是<全部>，则使用打印机时被禁止。

注意 只有打印机类型和打印机描述都匹配，“打印机”条件才算匹配。

6.16移动存储授权策略

为了方便管理企业内部使用的移动盘，防止企业内部机密资料通过移动存储设备外泄，管理员可以通过移动存储策略来授予不同的移动盘不同的权限，同时可以对复制到移动盘的文档进行加密，使其只能在企业授信的环境中才能打开。

设置策略前，管理员需要对企业内用到的移动盘进行合理的分类， 移动存储库的分类可参考后面的“**工具->分类管理->移动存储分类**”的说明文档。

移动存储设备的类型和操作权限包括：

策略属性名称	说明
加密盘类型	默认是“全部”，可以通过下拉列表选择加密盘或非加密盘；如果选择加密盘，则设置的策略只对所有的加密盘有效；
可读	允许任意程序以只读方式读取移动盘的内容，只有勾选此项，下面三项才有效。
自动解密	允许在资源管理器中从移动盘将文档复制到本地或者网络上时自动解密，而其他的应用程序读取移动盘上的文档不会自动解密；
可写	允许任意程序写到移动盘上，当不允许可写时，会禁止文档复制或保存到移动盘上，同时也会禁止删除，改名移动盘上的文档；只有勾选此项，自动加密才有效；
自动加密	禁止除了资源管理器之外的任何程序写数据到移动盘，当资源管理器复制文档到移动盘时，自动对文档加密。
移动存储类别	移动存储默认是<全部>，是指所有的移动存储设备，要设置指定的移动盘，只能到移动存储分类中选择，可以指定一个分类，也可以是具体的一个移动盘。

提示 如果企业想执行严格的移动盘控制策略，可以首先在整个网络中设置所有的移动盘都只读，不可写。
然后针对不同的部门和个人，设置其对不同的移动盘分类有不同的权限。比如每个部门都只能对属于自己部门的移动盘能够读写，而且读写时自动加密解密。
这样移动盘在部门内部使用是不受限制的，而且不会被其他部门的人读取数据，而那些外来的移动盘则只能读不能写。

注意 如果同时设置了文档控制策略和移动存储授权策略，则先执行文档控制策略，再执行移动存储授权策略。
例如允许读写移动盘，并且加密；而文档策略有禁止复制 word 文档到移动盘。则最后执行的结果是不允许复制 Word 文档到移动盘，而其他的文档复制到移动盘时会自动加密。

第七章 监视

7.1 即时通讯内容

即时通讯可以记录客户端机器上的聊天内容，为事后追查责任提供重要依据，及时发现非法的聊天内容，同时避免员工任意聊天而影响正常工作的情况。

支持的即时通讯工具

即时通讯记录支持各种聊天工具，包括：腾迅 QQ、TM、MSN Messenger、ICQ、Yahoo！Messenger、新浪 UC、网易 POPO、Skype、腾迅 RTX、Lotus Sametime 和贸易通 AliTalk。

其中，网易 POPO 暂时只能记录发送的消息内容。

即时通讯内容记录

即时通讯记录包含的内容有：

IM 内容字段	说明
聊天工具	记录使用的即时通讯工具；
本地账户	记录本地的即时通讯的账户昵称；
对方账户	记录聊天对方的账户昵称；
开始时间	该聊天记录的开始时间；
结束时间	该聊天记录的结束时间；
聊天语句数	统计聊天内容的语句数量，判断聊天内容的多少；
聊天内容	记录聊天的详细时间以及内容。

保存聊天内容

除了直接在控制台上查看聊天内容，管理员也可以将聊天内容保存起来，方便日后查询。

选中需要保存的聊天记录，单击右键“**另存为网页文件**”，将该聊天记录的所有聊天内容保存为 htm 或 html 文件。也可同时选中多个聊天记录，导出多个聊天内容，每个聊天记录以及内容会单独存放在一个文件中。

查询聊天内容

即时通讯内容可以按以下条件进行查询：

查询条件	说明
聊天工具	根据聊天工具查询，默认是全部，也可在下拉框中选择其中一种聊天工具进行查询；
用户 ID 或昵称	根据聊天双方的账户 ID 或昵称进行查询，查询指定账户的聊天记录及内容；
内容	根据聊天内容进行查询，可针对部分关键字进行快速定位，从而找到关心的聊天记录。

7.2 邮件内容

邮件记录会将客户端机器上使用邮件工具收发的邮件记录下来，以便管理员统一管理和掌握邮件内容，及时阻止非法的邮件内容。

邮件记录支持的邮件类型包括：普通邮件、Exchange 邮件、网页邮件、Lotus 邮件，其中普通邮件和Exchange邮件可以记录发送和接收，而网页邮件和Lotus邮件只能记录发送。

邮件记录内容

邮件记录包含的内容有：

属性名称	说明
发送/接收	表示发送的邮件记录， 表示接收的邮件记录；
主题	邮件的主题；
发件人	邮件的发件人的邮箱地址；
收件人	邮件的收件人的邮箱地址，包括抄送和暗送的邮件地址，在邮件记录的属性窗口中查看；
附件	“ ” 表示邮件有附件，邮件记录会自动备份附件文件，点击“ ” 按钮直接查看或保存附件文件；
大小	记录邮件的大小；
正文	选中一条邮件记录，在下面的视图中可以直接查看正文内容。

保存邮件内容

除了直接在控制台上查看邮件记录及内容，管理员也可以将邮件文件导出来保存。

选中一条邮件记录，单击右键“**另存为邮件文件**”将该邮件保存为 eml 文件，可以直接通过 outlook 打开并查看该文件。也可同时选择多个邮件同时导出保存。

查询邮件

可以按以下条件对邮件及内容进行查询：

查询条件	说明
邮件类型	根据邮件类型查询，默认是全部，也可在下拉框中选择其中一种邮件类型进行查询；
发送/接收	管理员可以只统计发送或接收的邮件；
邮件地址	根据邮件地址查询，查询指定邮件地址的邮件发送和接收情况；
主题	根据邮件主题查询，查询主题包含指定关键字的邮件记录；
内容	根据邮件内容查询，查询包含指定关键字的邮件，以帮助管理员快速定位关心的邮件内容；
包含附件	不勾选该项，查询到所有邮件记录(包含带附件和不带附件的邮件)，勾选该项，只查询包含附件的邮件；
附件名称	查询包含附件，且附件文件名称中包含指定关键字的邮件记录。
大小	设置邮件的大小范围，查询设置范围内的邮件记录。

7.3 实时屏幕

选择菜单“**监视->屏幕快照**”，管理员可以实时查看并跟踪某一台计算机或某一个用户的屏幕快照。

图标按钮	说明
	会话按钮，如果某台计算机登录了两个以上用户或某个用户同时登录两台以上计算机，管理员可以通过选择查看其中某一个的屏幕快照。
	适合窗口大小。
	原始大小。
	跟踪按钮，屏幕快照会自动刷新，刷新间隔时间在“**工具->选项->实时信息**”中查看和修改。
	停止跟踪，屏幕快照不会自动刷新。

选择了目标计算机之后，选择右键菜单“**跟踪**”对该计算机进行实时跟踪，图像区会不断地显示选定计算机的屏幕变化。当需要停止时，再选择右键菜单“**跟踪**”会停止跟踪。

7.4 多屏监视

多屏监视可以同时监控多台计算机的实时屏幕，多屏监视显示的是一个屏幕矩阵，这个矩阵的大小范围是（2 x 2）到（4 x 4）。选择菜单“**监视->多屏监视**”开始多屏监视。

设置监视矩阵的大小，系统自动在一定的时间间隔内更新屏幕快照，同时在到达一定的时间后轮转到下一批待监视的计算机，方便管理员同时监控多台计算机。

用户可以通过功能按钮快速查看最前一页、上一页、下一页和最后一页的计算机的屏幕快照；双击某一个被监控计算机的屏幕，可以对其进行全屏监视；还可以通过按钮“ ”选择需要监控的计算机或计算机组；

锁定位置

您可以在某一台计算机的屏幕的右键菜单里选中“**锁定位置**”使得在每一个多屏监视画面中都能看到该计算机的屏幕快照。被固定的计算机屏幕的标题是黄底黑字，假如您不想再固定该计算机的屏幕，您只要在该计算机的屏幕的右键菜单里钩选掉“**锁定位置**”恢复。

屏幕信息

鼠标移动到一个屏幕会显示当前客户端机器的屏幕信息，包括：计算机名称、网络地址、用户、状态。

7.5 查询屏幕历史

选择“**工具->查询屏幕历史**”默认查询的是当天的屏幕历史记录，只有设置了屏幕记录策略的客户端机器才能查询到屏幕记录。管理员也可以根据一定的查询条件快速找到需要的屏幕记录进行查看。

查询条件包括：

查询条件	说明
日期范围	设置开始日期和结束日期，查询一个时间段内的所有屏幕历史记录；
计算机名称	查询指定计算机名称的屏幕记录，支持模糊查询，如输入“TEC”，查询到所有计算机名称中包含“TEC”的计算机屏幕记录；
网络地址	输入指定的网络地址，查询该计算机的屏幕记录，可以输入一个 IP 地址，也可以输入一个 IP 地址范围，如：192.168.1.100-192.168.1.200。

查询到的屏幕记录日志包括：

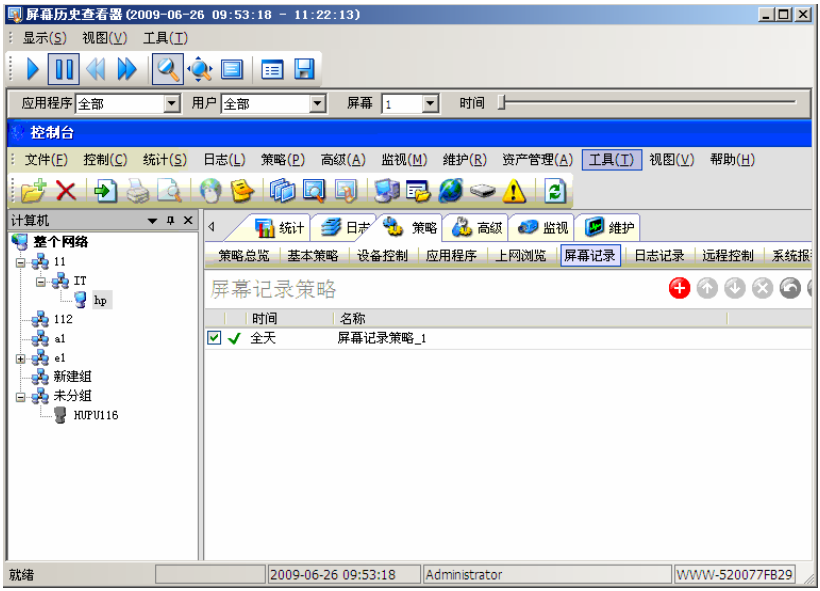
日志属性名称	说明
日期	屏幕记录的日期，屏幕记录以“天”为单位，一天的屏幕数据记录一个文件；
计算机	记录的客户端机器；
会话	会话 ID，如果只登录一个用户，则会话 ID 是 0，登录第二个用户，则会话 ID 是 1，如果登录过多个用户，则有多个屏幕记录，一个会话会记录为一个文件。 Vista 下第一个用户的会话 ID 为 1；
开始时间 结束时间	屏幕记录的开始时间和结束时间；
文件名称	如果屏幕数据是存放在 SQL 主数据库，则文件名称为<SQL>，如果屏幕数据存放在 SCREEN 目录下，则文件名称为其屏幕数据文件的名称，一般是以日期开头的字符串。

7.6 屏幕历史查看器

查询出需要查看的屏幕记录后，双击其中的一条记录或点击【查看】按钮打开屏幕历史查看器，查看该计算机的屏幕历史。屏幕查看器不能单独启动，只能从控制台模块中启动运行。

界面简介

屏幕历史查看器窗口包括：标题栏、菜单栏、工具栏、查询栏、时间刻度尺、图像显示区以及状态栏。



显示

可以通过菜单或工具栏上的按钮选择屏幕帧的位置，也可以直接拖动时间刻度尺上的滑块直接显示某一帧。

视图

管理员可以根据自己的需要在“视图”菜单选择是否显示工具栏、状态栏。同时类似于控制台模块中的图像区的显示方式，也有原始大小、按比例缩放和全屏幕。

播放速度

通过菜单“**视图->速度**”可以调节屏幕播放的速度。分为快、普通和慢三种速度，用户可以根据自己的需要选择播放速度。

查询

通过查询栏，管理员可以快速定位查询到需要的屏幕历史，可以分别根据应用程序、用户、屏幕和时间刻度尺进行查询。

查询项	说明
应用程序	默认播放所有应用程序的屏幕历史，也可从下拉菜单中指定一种应用程序，只播放该程序的屏幕历史；
用户	如果屏幕记录中记录了多个用户的屏幕历史，可以指定其中一个用户只查看该用户的屏幕历史；
屏幕	如果客户端机器有多个显示屏，则可以选择其中一个屏幕查看屏幕数据；
时间刻度尺	显示当前帧对应的时间，拖动滑块到指定的位置，查看当前帧的屏幕，鼠标停在上面时能显示该帧的基本信息。 选择菜单“工具->窗口标题变化”可查看每一帧的基本信息，包括：时间、用户、应用程序和标题。

导出为视频文件

管理员可将需要的屏幕历史保存起来，留作以后使用。选择“**工具->另存为视频文件**”，有 4 种保存方式，管理员可以指定其中一种方式保存屏幕历史。

保存方式	说明
按时间保存	保存一段时间内的屏幕数据，拖动时间刻度尺上的滑块，设置开始时间和结束时间；
按应用程序保存	只保存指定的应用程序对应的屏幕历史记录；
按用户保存	只保存指定的一个用户对应的屏幕历史记录；
全部保存	保存所有的屏幕历史。

第八章 远程维护

IT 人员为 PC 做简单的日常维护工作所花的时间占其总工作量的 70-80%，大大增加计算机网络的综合管理成本。而且如果问题没有得到及时有效的处理，也会极大影响企业的生产力。因此有必要减少 IT 人员的一些无谓操作，大幅度提升他们的工作效率，使得 IT 人员更加关注于管理工作，并将精力集中于能够提升企业管理效率的信息系统中。

Viacontrol 能帮助 IT 人员实时查看远程计算机的信息，帮助分析和解决远程计算机的故障。

8.1 远程维护

8.1.1 应用程序列表

选择菜单“**维护->应用程序**”可以实时查看客户端机器的应用程序列表，查看当前启动的所有任务以及状态信息，其中当前激活的应用程序名称用深蓝色粗体字显示。

图标按钮	说明
	会话按钮，如果客户端机器登录多个用户，单击该按钮选择不同的用户查看其应用程序列表；在用户模式下，如果该用户在多个计算机上登录，单击该按钮选择不同的计算机查看应用程序列表。
	跟踪按钮，应用程序列表会自动刷新，时间间隔在“**工具->选项->实时信息**”中设置和查看。

结束任务

管理员可以在控制台上远程结束应用程序任务，选择需要结束的应用程序，单击右键“**结束任务**”确定后关闭指定的应用程序。

8.1.2 进程列表

选择菜单“**维护->进程列表**”可以实时查看客户端机器上的所有当前进程，进程信息包括：文件名称、PID、时间、会话 ID、CPU、CPU 时间、内存、虚拟内存、基本优先级、句柄数、线程数以及路径。

字段名称	说明
时间	该进程的启动时间；
路径	该进程所在客户端机器上的详细路径；
其它	其它各列属性与操作系统任务管理器的进程页中的各属性含义相同。

进程列表的各列属性可以帮助管理员分析是否有非法的进程或病毒并尽快解决问题。

图标按钮	说明
	会话按钮，只在用户模式下有效，选择查看不同的计算机的进程列表；
	跟踪按钮，与应用程序列表中的含义相同。

结束进程

管理员可以在控制台上远程结束指定的进程，选择需要关闭的进程，单击右键“**结束进程**”关闭客户端机器上的进程。

8.1.3 性能

选择菜单“**维护->性能**”可以远程实时查看客户端机器的各种性能，包括：CPU 的使用率、内存的使用率等。其中，总数、物理内存、认可用量、核心内存的值是客户端机器上的【任务管理器】->【性能】中的数据。

图标按钮	说明
	会话按钮，只在用户模式下有效，查看不同计算机的性能列表；
	跟踪按钮，与应用程序列表中的含义相同。

8.1.4 设备管理器

选择菜单“**维护->设备管理器**”可以实时查看客户端机器上的设备列表，包括：处理器、磁盘驱动器、存储卷、键盘、鼠标、网络适配器等各种计算机硬件设备。

图标按钮	说明
	设备列表的查看方式，包括：按类型查看、按连接查看以及是否显示隐藏的设备；
	只在用户模式下有效，选择查看不同计算机的设备。

禁用/启用设备

管理员可以在控制台上远程禁用/启用设备管理器中的硬件设备，选择需要禁用/启用的设备，单击右键“**禁用**”或“**启用**”来远程操作客户端机器的设备。

8.1.5 系统服务

选择菜单“**维护->系统服务**”可以实时查看客户端机器的系统服务列表信息，包括：名称、描述、状态、启动类型、登录身份、路径。

图标按钮	说明
	只在用户模式下有效，选择查看不同计算机的系统服务

远程操作

管理员可以像在本地操作一样设置和更改服务的状态以及启动类型。选择需要设置的服务，单击右键“**启动/停止**”更改服务的状态，右键“**启动类型->自动/手动/禁用**”中选择需要设置的启动类型。

8.1.6 磁盘管理

选择菜单“**维护->磁盘管理**”可以实时查看客户端机器的磁盘分区列表以及使用情况，包括的内容有：卷标、文件系统、容量、空闲空间、%使用。

图标按钮	说明
	只在用户模式下有效，选择查看不同计算机的磁盘管理

8.1.7 共享文件夹

选择菜单“**维护->共享文件夹**”实时查看客户端机器的共享情况，包括：网络共享、会话、打开文件。

图标按钮	说明
	网络共享视图按钮；
	会话视图按钮；
	打开文件视图按钮；
	只在用户模式下有效，选择查看不同计算机的共享信息

网络共享

管理员通过查看网络共享可以知道客户端机器开启了哪些共享文件，并可以根据安全需要实时关闭一些共享，选择需要关闭的共享，单击右键“**停止共享**”关闭该共享文件。

会话

单击“显示”按钮选择“会话”模式可以查看客户端机器上的共享文件是否有远程机器访问，并且访问共享的远程机器的情况，包括：用户、计算机、类型、打开文件、连接时间、空闲时间、是否来宾。

假如管理员发现非法的访问连接，可以实时关闭该连接，选择该会话，单击右键“**关闭会话**”暂时关闭该会话。

打开文件

打开文件列表是远程机器访问客户端机器共享文件的列表，包括：打开文件、访问者、锁定、模式。

管理员也可以通过右键“**将打开的文件关闭**”或“**中断全部打开的文件**”实时关闭一个或所有的打开的文件。

8.1.8 计划任务

选择菜单“**维护->计划任务**”可实时查看客户端机器上的计划任务列表，包括：名称、计划、应用程序、下次运行时间、上次运行时间、状态、上次结果以及编写者。

管理员可直接通过控制台删除非法的计划任务，选择需要删除的计划任务，单击右键“**删除**”实时删除指定的计划任务。

图标按钮	说明
	只在用户模式下有效，选择查看不同计算机的计划任务

8.1.9 用户和组

选择菜单“**维护->用户和组**”可实时查看客户端机器的所有本地用户以及用户组。

本地用户列表包括：用户名称、全名以及描述。

用户组列表包括：组名称以及描述。

图标按钮	说明
	只在用户模式下有效，选择查看不同计算机的用户和用户组。

8.2 远程控制

8.2.1 远程控制

远程控制是通过控制台远程操作客户端机器，为网络管理提供方便，帮助管理员远程查看机器故障，快速解决系统问题。

选定目标计算机，选择菜单“**维护->远程控制**”，远程控制有 2 种授权方式：用户授权和密码授权。

用户授权

选定目标计算机，选择菜单“**维护->远程控制**”，控制台会弹出确定请求远程用户授权的提示框，点击“是”，目标客户机会弹出对话框询问当前用户是否允许控制台对其远程控制。如果用户允许，则进入控制界面，否则控制结束。

密码授权

选定目标计算机，选择菜单“**维护->远程控制**”，控制台会弹出对话框要求输入密码，密码正确，则进入控制界面，否则控制结束。
远程控制密码要在客户端机器上设置，方法是 shift+alt+ctrl+ “ocularrm” 会弹出密码设置框，输入密码即可。

设置了密码的客户端机器，也可以通过用户授权的方式进行远程控制。但是如果策略设置了允许远程控制并且需要强制确认，只能通过用户授权的方式来控制。

远程控制界面

当进入远程控制的状态时，目标计算机的右上方会显示“**Remote Controlling...**”。

通过工具栏按钮，可以选择屏幕缩放的比例，以及是否全屏幕控制。在全屏幕控制时，如果需要退出全屏显示，可直接按 F12 键。

按钮“ ”可以控制显示色彩在 256 色和真彩色之间转换。

按钮“ ”可以对目标计算机的键盘和鼠标设置锁定和解锁；

按钮“ ”可以控制是否允许在控制台与目标计算机之间进行剪贴板操作；

如果需要向受到远程控制的计算机使用 Ctrl-Alt-Del、Ctrl-Esc 或 F12，您可用鼠标右击 Viacontrol 远程控制窗口的标题列或在 Windows 工具列上远程控制窗口的图标，并在弹出的菜单选择 “Send Ctrl-Alt-Del”、“Send Ctrl-ESC”或“Send F12”。

8.2.2 远程文件传送

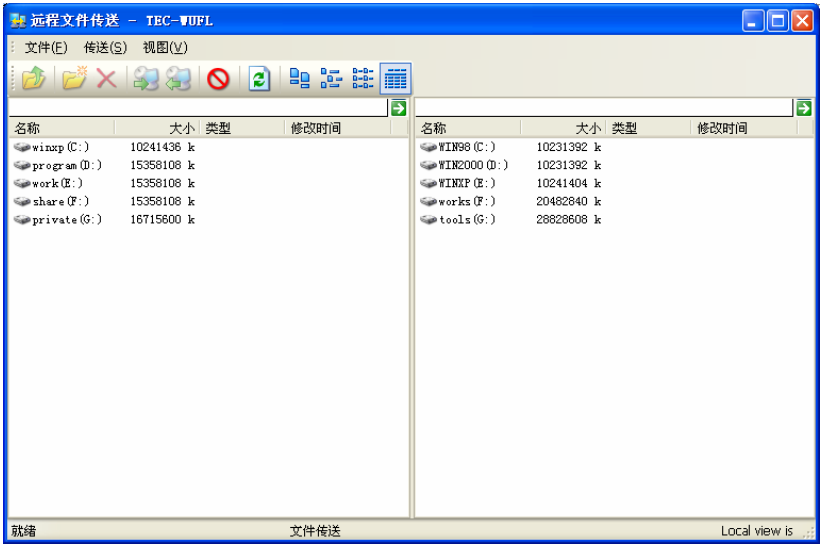
远程文件传送是指在控制台机器和目标客户端机器之间的文件传送，通过远程文件传送功能，管理员可以快速分发文件到目标计算机，提高工作效率。

远程文件传送和远程控制一样，有 2 种授权方式：用户授权和密码授权，控制台获得用户授权后，进入远程文件传送窗口。

界面介绍

远程文件传送窗口包括：标题栏、菜单栏、工具栏、本地资源视图、远程资源视图以及状态栏。

其中本地资源视图是控制台机器的资源信息，远程资源视图是远程客户端机器的资源信息。双击文件夹进入下一级目录，也可以直接在地址栏中输入文件的路径来查找文件。



文件操作

管理员可以直接双击进入下一级目录，也可以在地址栏中直接输入路径来查找文件，选择“**文件->向上**”返回上一级目录。同时可以对文件做一些简单操作，包括新建文件夹、重命名、删除，地址栏为空也就是在根目录下无法进行这些文档操作。

远程视图和本地视图操作相同。

文件传送

传送功能	说明
本地到远程	选中本地机器需要传送的文件，选择菜单“**传送->本地到远程**”就可以把选中的文件传送到远程目标计算机；
远程到本地	选择远程机器中需要传送的文件，选择菜单“**传送->远程到本地**”复制远程文件到本地计算机；
终止传送	在文件传送过程中选择菜单“**传送->停止**”可以终止文件传送，状态栏会显示文件传送失败。

本地视图和远程视图之间支持拖拽传送文件，可同时选择多个文件进行传送，正在文件传送时不能进行其他操作。

显示模式

本地与远程视图均支持大图标，小图标，列表，详细信息等显示模式。单击工具栏上的显示图标选择合适的排列方式。

注意 需要传送文件时，本地视图和远程视图都不能为根目录，否则不能传送文件。

第九章 资产管理

9.1 资产管理

资产管理功能搜集了所有客户端机器的软、硬件资产信息，方便管理员对企业内部的软硬件资产的维护和查看，并提供了各种查询条件，更方便了对各种资产的统计。

选择菜单“**资产管理->资产管理**”进入资产管理主窗口。资产管理窗口包括：标题栏、菜单栏、工具栏、任务导航栏、数据显示区、状态栏。

9.1.1 资产类别及资产属性说明

资产类别

资产的类别包括：

类别	说明
计算机类	是对客户端所在计算机的一些概要性的描述，如登录用户、域、机器名称等。
硬件类	是客户端机器的所有硬件设备，包括 CPU、内存、硬盘、主板、网卡等。
软件类	是客户端机器的软件类别，包括：操作系统、应用软件、杀毒程序、Windows 系统软件、微软产品补丁。
自定义类别	由客户自定义的无法自动获取的资产（如交换机，路由器，办公桌等）

资产属性

对于每一种资产，我们可能会有多个属性来描述它。比如对于内存有名称、插槽、容量、最大容量、内存条类型（如 DDR、SDRAM 等）；而对于硬盘我们会有名称、序号、容量等。

属性包括类别属性和实例属性

属性类型	说明
类别属性	是资产的统计属性，属于这个类，比如针对内存，会有其类别属性如内存总容量、最大容量和内存条数量等。
实例属性	是指这个资产类的一个实例的属性，比如内存是一个资产类，内存可以有多个，而针对每一个内存有其实例属性，如插槽、容量、类型等。

计算机类只会有类别属性(因为计算机始终只有一个)。
硬件和软件资产包含有类别属性和实例属性。
自定义类别只会有实例属性(因为这些都是用户自己定义的)。

9.1.2 资产类别管理

资产类别管理中会列出所有的资产类别及其各种属性，管理员可以通过资产类别管理查看某一种资产的所有属性，也可以手工添加资产属性。

选择菜单“**资产管理->资产类别管理**”打开资产类别管理窗口，左边视图是所有资产的树形结构，显示类别树，而右边视图是该资产的属性列表。在属性列表中，黑色字体的属性为类别属性，蓝色字体的属性为实例属性。

属性的值类型

属性有 5 种类型，用不同的图标表示。

图标	类型
	文字
	整数
	小数
	日期
	是/否

自定义属性

除了系统为各种资产定义的属性，管理员可以手工自定义属性。

假如需要新增一个 CPU 的实例属性“保修期”，在 CPU 右边的属性列表区域，选择菜单“**操作->新建属性**”打开资产属性编辑框，选择属性类型为“实例属性”，输入资产属性名称“保修期”，指定值类型为“日期”，单击【确定】

按钮。

自定义的资产属性名称后加星号“*”标识。自定义的属性可以选择菜单“**操作->重命名**”或“**操作->删除**”来修改，但是系统默认的资产属性不能重命名和删除。

自定义资产

管理员可以自定义资产，将企业内的其它资产记录起来，方便随时查看和统计。

例如，企业内有 3 台打印机，管理员可以自定义资产“打印机”并且添加其属性值。选择菜单“**操作->新建资产**”输入资产名称为“打印机”，为打印机添加实例属性：型号、部门、购买日期、价格等。

对于自定义的资产，需要管理员手工添加这些属性值，属性值在菜单“**资产管理->其它资产**”中添加，详细说明请参考小节 9.1.7 其它资产。

9.1.3 硬件资产查询

选择菜单“**资产管理->硬件资产**”可以查看客户端机器的所有硬件资产，也可以根据需要查询统计各类资产。

查看资产信息

系统默认统计所有客户端机器的 CPU、内存、硬盘驱动器和网卡概述信息，选择需要查看的计算机，单击右键“**属性**”或直接双击查看单个计算机的硬件资产信息。

资产信息窗口会默认显示计算机类和硬件类的资产信息，类似资源管理器，左边树形结构，显示类别树，右边是列表结构，显示属性内容。选择菜单“**显示->所有类别信息**”或“**显示->软件类别信息**”也可查看其它资产信息。

在资产实例属性中，有个默认属性【摘要】是对该资产实例的摘要信息，也是显示在资产类别树中的名称；在所有的类别属性中，有个默认属性【概述】是对所有实例的摘要的汇总。

提示 查看资产信息时，可以直接为自定义资产属性添加值。找到自定义的属性，选择菜单“**操作->属性**”打开资产属性编辑框，输入内容添加属性值。

查询资产

管理员可以设置一个或多个查询条件来统计需要查看的结果，单击资产结果列表右上方的查询按钮“”打开查询条件设置框，设置查询条件：

查询条件	说明
范围	默认是{整个网络}内所有的客户端机器，单击右边的“...”按钮只选择其中一个计算机组
	添加按钮，单击该按钮打开条件设置对话框，每个条件包括：资产属性、运算符和内容，如：内存-数量 == 2 是一个查询条件，CPU-名称 包含 “AMD”也是一个查询条件
	删除设置的查询条件
	查看并修改查询条件
满足任何一条即可	选中该项，则满足任何一个查询条件即可；不选中该项，则需要同时满足所有的查询条件

注意 设置查询条件时，如果一个条件中包含了某一个资产 A 的实例属性，再添加条件时就不可以再包含另一个资产 B 的实例属性，只能再添加类别属性的条件。

设置了查询条件后，添加结果列表，选择需要显示的资产属性。

图标按钮	说明
=>	在左边的资产类别树中选择需要显示的属性直接双击或单击该按钮移动到结果列表中
<=	将资产属性从结果列表中移出，可同时选择多个移出

注意 结果列表和查询条件一样，如果已经包含一个资产 A 的实例属性，无法再添加另一个资产 B 的实例属性。

设置好查询条件以及结果列表后，为了方便日后查询，可以将当前的设置保存或设置为默认，也可以删除不要的查询设置。

操作	说明
保存	输入保存的名称，单击【保存】按钮，下次需要使用时，直接从名称下拉框中找到输入的名称调出之前的设置；
删除	单击【保存】按钮，删除已经保存的查询设置。
设为默认	管理员可以更改查询设置并将其设为默认查询，单击【设为默认】按钮，则以后重新打开资产管理窗口，都显示的是默认查询结果

编辑自定义属性内容

以前面提到的自定义属性“CPU-保修期”为例，设置查询条件：“CPU-保修期”为“不存在”，结果列表：“计算机-概述”，“CPU-摘要”，“CPU-保修期”，查询结果可以看到“CPU-保修期*”列的内容都为空，选中一行记录，点击该列的区域，鼠标成可编辑状态，输入属性内容，该属性内容会保存到数据库。可依次添加其他的该属性值。

注意 结果列表中必须包含“CPU-保修期”，除此之外，由于“CPU-保修期”是自定义实例属性，所以结果列表中还必须包含 CPU 的其它任意一个实例属性，否则无法编辑属性值。

9.1.4 硬件资产变更

硬件资产变更记录了所有客户端机器的硬件资产的变化情况，包括增加、删除和变化。选择菜单“**资产变更->硬件资产变更**”查看所有硬件资产变更记录。

查看资产变更内容

硬件资产变更记录包含的内容有：变更类型、时间、计算机、资产类别、描述。

字段名称	说明
变更类型	资产的变化类型，包括增加、删除、变化；
资产类别	发生变化的资产类别；
描述	发生变化的描述信息，右键单击变更记录**“属性”**中可以查看详细信息，包含了资产的各属性内容的变更。

查询资产变更

选择菜单“**文件->新建查询**”打开硬件资产的查询栏，管理员可以设置各种查询条件来有针对性地查询：

查询条件	说明
时间和范围	通用查询条件；
类型	硬件资产类别，默认是全部，也可以在下拉框中指定其中一种资产进行查询；
内容	根据描述信息查询，支持模糊查询。

9.1.5 软件资产查询

选择菜单“**资产管理->软件资产**”切换到软件资产查询，默认查询计算机以及操作系统，管理员可以设置其它查询条件查询需要的结果。

软件资产查询类似与硬件资产查询，请参考硬件资产查询的说明。

9.1.6 软件资产变更

软件资产变更记录了所有客户端机器的软件变化情况，包括：增加、删除和变化。选择菜单“**资产管理->软件资产变更**”查看所有软件资产变更记录。

软件资产变更记录的内容与硬件资产变更记录类似，查询条件包括：

查询条件	说明
时间和范围	通用查询条件；
类型	软件资产的类别，包括：操作系统、应用软件、杀毒软件、Windows 系统软件、微软产品补丁；
内容	根据描述信息查询，支持模糊查询。

9.1.7 其它资产

管理员在资产类别管理中定义了资产类别以及资产属性后，需要在“**资产管理->其它资产**”中添加资产属性内容。

添加自定义资产

以前面定义的“打印机”为例，选择菜单“**文件->新建查询**”打开查询条件框，查询条件为空，结果列表为：打印机-型号、打印机-部门、打印机-购买日期、打印机-价格，查询出打印机的所有属性。

单击查询结果列表右上方的添加按钮“ ”输入第一台打印机的各种属性值，再依次添加记录，输入第二台和第三台打印机的属性值。打印机的属性记录会保存起来，方便日后查询。

查询自定义资产

添加保存自定义资产的属性值后，也可以建立查询条件，选择菜单“**文件->新建查询**”设置查询条件，如：“打印机-价格” >= 1000，结果列表：打印机-

型号、打印机-部门、打印机-购买日期、打印机-价格，则只查询出价格在 1000 元以上的打印机。

9.2 补丁管理

补丁管理功能可以扫描出所有客户端机器的补丁安装情况，并且根据需要为客户端机器自动安装补丁，增强系统安全性，也节约企业下载成本，提高网络管理员的工作效率。

补丁的扫描、下载和安装

在安装服务器的机器上同时运行着补丁下载器，它会自动下载并更新补丁检测文件(wsusscan.cab)。客户端第一次安装后会自动从服务器下载补丁检测文件，一般在客户端启动半小时后自动检测补丁的安装情况。

如果对补丁安装没有特别要求，需要所有的客户端都自动安装补丁，可以在第一次启动控制台时，在菜单“**工具->选项->服务器设置->补丁选项**”中勾选“**新出现的客户端默认自动安装**”或“**新出现的补丁默认自动下载**”。如果在客户端的补丁扫描已经完成再设置这 2 个选项，则只对以后扫描到的补丁和新加入的客户端生效。

管理员可以在控制台上选择菜单“**资产管理->补丁管理**”来查看客户端机器的补丁安装情况。

如果没有在“**工具->选项->补丁选项**”中设置“自动下载”和“自动安装”，则需要管理员为补丁设置下载策略来下载补丁到服务器，同时设置需要安装补丁的计算机，客户端机器会根据设置从服务器中获取补丁安装文件并且自动安装。

提示 设置下载策略和安装策略时可结合 CTRL 和 SHIFT 键，同时对多个补丁或计算机设置策略。

控制功能

管理员可以在控制台上直接下达扫描或下载补丁的命令，在列表视图的右上方有一个命令按钮“ ”和范围按钮“ ”。点命令按钮，可以选择下载检测文件，下载所有补丁和检测整个网络系统补丁。

控制功能	说明
下载检测文件	选择“**下载检测文件**”，服务器会立即下载最新版本的补丁检测文件；
下载所有补丁	选择“**下载所有补丁**”，服务器会立即下载设置了下载策略的补丁；
检测整个网络系统补丁	选择“**检测整个网络系统补丁**”，所有的客户端机器会立即扫描一次补丁；
检测系统补丁	假如只需要立即扫描一台机器的补丁，右键单击计算机信息，选择菜单“**检测系统补丁**”，则只会立即扫描指定的客户端机器的补丁；
选择计算机范围	点击范围按钮可选择查看一个计算机组或单个计算机的补丁安装情况。

9.2.1 按补丁模式查看

补丁日志内容

按补丁模式查看可以查看由客户端机器上扫描出来的所有补丁列表，补丁记录包括：

属性名称	说明
严重级别	补丁本身的级别，包括：低、中等、重要、严重和未知。
公告号	微软发布的补丁的公告号。
补丁 ID	补丁 ID。
名称	补丁的名称，一般也包含了补丁 ID。
未安装数量	需要安装该补丁但是没有安装的客户端机器的数量，选择该补丁，在下面的计算机列表中可以查看已安装和未安装的计算机。
下载策略	管理员设置的该补丁的下载策略：下载/不下载，不下载该列为空，服务器不会自动下载这个补丁。选择该补丁，右键可以设置下载策略。
下载状态	补丁的下载状态，包括：未下载、下载中、已下载，鼠标移动到一个补丁，会自动显示该补丁的下载进度，下载完成为 100%。
详细信息	双击或右键单击一个补丁“详细信息”可以查看补丁的其它信息，包括：下载路径、补丁大小以及补丁的描述信息。

补丁下载设置

在补丁模式下查看到所有客户端机器的补丁列表。如果之前没有设置“新出现的补丁默认自动下载”，则管理员需要手工设置。

右键单击补丁信息，设置“下载/不下载”，设置了“下载”的补丁服务器会自动下载，下载策略中用“✔”表示；设置了“不下载”的补丁服务器不会自动下载，下载策略中内容为空。

对于以后出现的补丁，也可以设置是否自动下载。在控制台主菜单“**工具->选项->服务器设置->补丁选项**”中可以设置【新发现的补丁默认自动下载】。

9.2.2 按计算机模式查看

计算机日志内容

按计算机模式查看可以查看所有客户端机器的信息以及补丁安装情况，计算机信息包括：

属性名称	说明
计算机	客户端机器的分组和计算机名称；
网络地址	计算机的 IP 地址；
操作系统	计算机的操作系统；
最后扫描时间	计算机的补丁扫描的最后时间；
安装策略	是否自动安装补丁。

计算机补丁安装设置

在“**补丁管理->计算机模式**”下显示了客户端机器列表以及补丁安装明细。如果之前没有设置“新出现的客户端默认自动安装”，则管理员需要手工设置。

右键单击计算机信息，设置“**安装/不安装**”，设置了安装的计算机会自动安装下载了的补丁；设置不安装的计算机不会自动安装补丁。

管理员也可以针对单个计算机的部分补丁单独设置安装策略，在指定计算机的补丁明细列表中选择补丁记录，右键设置“安装/不安装”。

在控制台主菜单“**工具->选项->服务器设置->补丁选项**”中可以设置【新发现的客户端默认自动安装】。

9.3 漏洞检查

漏洞检查功能自动扫描网络内的计算机的漏洞并进行统计，方便网络管理员查看及统计计算机漏洞，并针对这些漏洞及时采取应对措施，修复计算机漏洞，增强计算机的安全性。

安装了客户端的计算机会自动扫描漏洞信息，管理员也可以在控制台上下达扫描命令立即扫描，单击命令按钮“ ”立即执行漏洞检查，单击范围按钮“ ”可以选择查看一个计算机组或单个计算机的漏洞信息。

9.3.1 按漏洞模式查看

在“**漏洞检查->漏洞模式**”下可以查看漏洞列表以及哪些计算机有漏洞，漏洞列表包含的内容有：

属性名称	说明
严重级别	漏洞的级别，包括：信息、一般和严重；
名称	漏洞的名称摘要；
有漏洞数量	存在该漏洞的客户端机器的数量；
无漏洞数量	没有该漏洞的客户端机器的数量；
其它详细信息	右键单击一个漏洞信息“详细信息”中可以查看该漏洞的详细描述信息以及解决方法，管理员可以根据解决方案手工修复漏洞。

9.3.2 按计算机模式查看

在“**漏洞检查->计算机模式**”下查看计算机信息以及漏洞明细。
计算机信息包括：计算机、网络地址以及操作系统；
漏洞明细包括：严重级别、名称、有无漏洞。

双击某个漏洞，可查看漏洞的详细信息及解决方法。

9.4 软件分发

通过 Viacontrol 控制台，管理员可以向客户端自动分发及安装软件，或者复制特定的文件或应用程序到客户端，透过使用软件分发功能，管理员能迅速地对整个网络的软件使用和业务应用做统一的部署，大大减轻了管理员的负担。

选择菜单“**资产管理->软件分发**”管理员可以建立分发任务。分发过程分为两步：创建分发程序包和创建分发任务。分发任务会把做好的程序包分发到指定的客户端上。

9.4.1 分发程序包

管理员需要首先创建分发程序包，分发程序包设置了该程序包进行分发时需要的参数信息，保存在服务器上，可以重复使用。

点击新增按钮“ ”新建一个分发程序包，创建分发包需要设置的信息包括：常规信息、文件信息、检测条件和必要条件。

设置常规信息

首先设置常规信息，包括：

字段名称	说明
程序包名称	程序包名称默认为“新程序包”，管理员可以修改名称，但是不能为空；
创建时间 修改时间	这两项都是系统自动生成的，不能编辑，新建时为空，创建完成再查看或者编辑时就可以看到创建时间和管理员名称；如果修改了该程序包，修改时间也会跟着变化；
操作系统	选择该程序包有效的操作系统，可以选择多个，默认全选；
系统语言	选择一种该程序包有效的系统语言，默认选择“全部”。

设置文件信息

在左边视图中切换到“文件信息”设置文件信息，包括：

字段名称	说明
常规	包括程序包大小、所在计算机、原始路径。
程序包大小	程序包创建后的大小（只读）；
所在计算机	创建该分发程序包时控制台所在的计算机名称（只读）；
原始路径	该分发程序包文件的原始路径（只读）；
分发模式	包括安装软件，执行程序和派发文件三种方式。
安装软件	派发应用软件安装程序到客户端机器并且安装；
执行程序	在客户端机器执行且仅执行一次指定的程序；
派发文件	派发指定的文件到客户端机器上；
命令行	当分发模式是“安装软件”或“执行程序”时，需要设置命令行参数。 安装软件模式的命令行一般为核心安装文件的名称，执行程序模式的命令行为执行程序的文件名称。 可以手工输入命令行，也可以在下面的文件列表中选择要执行的安装文件或程序，右键提取文件名为命令行。
目标路径	当分发模式是“派发文件”时，需要设置文件包的目标路径，即文件被派发到目标计算机的详细路径。目标路径默认为“{sd}\deploy files”，即客户端系统盘上的“deploy files”目录。
运行模式	“在用户桌面上运行”是指安装过程要与使用者交互，使用者可以看到安装过程和执行程序的界面。 不选中“在用户桌面上运行”则是静默安装，用户看不到安装过程和执行的程序，但是如果安装程序本身不支持静默安装，需要和使用者交互的话，安装程序将会停在界面中等待交互，从而导致安装失败。
文件列表	显示程序包中的各个文件和目录。文件列表信息包括：文件名称、文件大小、修改时间以及版本信息。 点击列表右上方的新增按钮“ ”，选择需要分发的文件(文件夹)，可同时添加多个文件和文件夹，但是这些文件和文件夹必须在同一个父文件夹内。 每次点击新增按钮选择文件时都是重新创建一个新文件列表，会自动覆盖掉之前选择的文件列表。

设置检测条件和必要条件

检测条件是检查软件是否成功安装的标准，客户端会自动检测此条件，如果满足条件则认为软件安装成功，否则会继续尝试安装。“安装软件”模式必须设置检测条件，其它分发模式不需要设置。

必要条件是执行本程序包所必须具备的条件，在派发程序包之前检测该条件，条件满足才派发，否则不派发，此条件是可选配置。

针对不同的系统软件环境的判断，检测条件或必要条件的设置有 5 种类型：

检测条件	说明
文件	判断某个文件是否存在，需要输入全路径；
文件版本	判断文件以及版本，需要输入全路径；
注册表项	判断某个注册表项存在；
注册表值	判断某个注册表项以及注册表值作更详细的定位；
安装的软件	一般是指在“**控制面板->添加/删除程序**”中的程序名称。

检测条件实例：

下面是制作安装 Microsoft Office 2003 程序包的检测条件

条件类型	逻辑	内容
文件	存在	%pf%\Microsoft Office\OFFICE11\EXCEL.EXE
文件版本	>= 11.0.5612.0	%pf%\Microsoft Office\OFFICE11\EXCEL.EXE
注册表项	存在	SOFTWARE\Microsoft\Office\11.0\Access\ InstallRoot
注册表值	存在	SOFTWARE\Microsoft\Office\11.0\Access\ InstallRoot – Path
安装的软件	包含	Microsoft Office Professional Edition 2003

提示 条件的指定文件路径的字符串可以包含预定的宏，如:

"tmp" temp folder(c:\windows\temp)
"win" windows directory(c:\windows)
"sys" system directory(c:\windows\system32)
"pf" program files(c:\program files)
"sd" system drive(c:\)
"cf" common files(c:\program files\common files)

程序包的删除和修改

删除操作是将程序包删除，编辑操作是修改程序包的参数，条件等信息。只有当程序包的状态为“准备就绪”时才可以对程序包进行删除和修改；当没有使用该程序包的分发任务时，该程序包处于“准备就绪”状态。

9.4.2 分发任务

创建了分发程序包后，还需要创建分发任务来指派目标计算机。在分发任务视图中点击右上方的新建按钮“ ”创建一个分发任务。

分发任务的设置包括：

字段名称	说明
任务名称	默认名称是“新任务”，管理员可以修改，名称不能为空。
程序包名称	点击“...”按钮选择需要使用的分发程序包。
最多重试次数	分发任务失败后会尝试重试，重试次数默认是“10”，也可以修改为其它整数（输入 0，则分发任务除非中止，否则如果失败会一直重试下去，直到分发能够成功）。
目标计算机	点击“ ”按钮选择分发任务的目标客户端计算机。

任务属性设置好后点击【确定】，分发任务立即启动，在任务列表中可以查看任务分发情况。

分发任务也有删除和编辑操作。在任务分发过程中，不能删除和编辑，必须先停止该任务的分发（可以单击某个分发任务，右键选择“停止”），然后再进行删除和编辑。

注意 如果分发任务在进行列表中使用的程序包的状态为“程序包正在使用中”，不能删除和修改，只有将分发任务删除，对应的分发程序包的状态才会变为“准备就绪”。

第十章 网络接入检测

网络接入检测功能可以发现是否有非法的计算机接入网络，并且对其进行网络阻断，有效保护网络内的机密文件，防止外来计算机接入网络窃取资料，同时也可以减少病毒的入侵，增强企业内计算机的安全性。

选择菜单“**工具->网络接入检测**”打开网络接入检测窗口。

10.1启动接入检测

启动接入检测

网络接入检测默认并没有打开，所以刚开始接入检测窗口的内容为空。要启动接入检测，选择“**操作->设置**”设置接入检测策略。

在设置对话框中勾选“启动接入检测”，则客户端会启动接入检测功能，安装了客户端计算机的网段内所有在线的计算机都会被扫描出来。在每个网段内会有一个客户端机器作为检测代理，用小红旗标识，作为检测代理的计算机会扫描其所在网段内所有的计算机。

如果启动接入检测的同时设置了“检测 IP 地址范围”，则只会扫描 IP 地址属于设置的 IP 地址范围内的网络设备，前提是这个 IP 地址范围内有安装了客户端模块的机器。

新扫描到一台计算机时，控制台上会有报警信息，已经出现在计算机列表中的机器则不会再报警。

计算机类型及设置

自动扫描出来的计算机有 2 种类型：正常和未知，同时管理员可以手工为这些计算机指定类型，包括授权、保护、非法：

计算机类型	说明
正常	表示安装了客户端模块的计算机；
授权	设置为授权的计算机不会被阻断，可将网络内管理者的计算机或关键网络设备设为授权，防止因为没有安装客户端被认为是“非法”计算机；

计算机类型	说明
保护	一般是将网络内重要的计算机设置为保护，以阻断非法计算机访问并窃取机密资料。
非法	设置为非法的计算机，当设置了启动接入控制功能后，会对其进行阻断，禁止它与保护的计算机之间的通讯。
未知	没有安装客户端模块的计算机，同时也没有手工指定其类型，当“**操作->设置**”中勾选了“阻止未设定标志并没有安装客户端的计算机访问受保护的计算机”时，会被认为是“非法计算机”并对其进行网络阻断，禁止它与被保护的网络设备之间的通讯。

提示 设置计算机类型时，可同时选择多个计算机进行同时设置。

10.2启动接入控制

启动接入控制功能

设置好计算机的类型后，可以启动接入控制功能。选择“**操作->设置**”打开策略设置对话框。

1) 启动接入控制功能

如果选中此项，代理计算机将启动接入控制功能，阻断“非法”的计算机访问“保护”的计算机。

管理员可将不允许访问“保护”的计算机都设置为“非法”。

2) 未设定标志并没有安装客户端的计算机访问受保护的计算机

如果勾选此项，“未知”的计算机也会被阻断，不能访问“保护”的计算机，设置此项前，请确认“未知”的计算机都需要被阻断，否则，请手工指定其类型。

一般来说，外来接入的计算机被检测到的类型都是“未知”，因而无法访问“保护”的计算机，达到保护企业机密资料的目的。

3) 阻止 IP 地址范围

如果不设置阻止 IP 地址范围，代理计算机会对网段内所有非法计算机进行阻断；如果指定了 IP 地址范围，则只会对设置范围内非法的计算机进行阻断。

10.3其它设置功能

设置检测代理

有小红旗标志“ ”的计算机是检测代理，检测代理负责扫描本网段内所有在线的计算机，并且执行控制功能，阻断非法的计算机。

为了方便管理网络内的计算机，管理员可以指定一台或几台稳定的客户端机器（例如没有安装个人防火墙且不经常关机的机器）优先成为检测代理。这样，只要这些机器正常运行，它们其中的一台就能成为检测代理。

选择“**操作->设置为检测代理**”指定检测代理，用蓝色小旗“ ”表示，只有类型为“正常”的机器才可以设置为检测代理。设置为检测代理的计算机将优先成为检测代理。

选择“**操作->禁止成为检测代理**”管理员可以指定部分计算机不能成为检测代理，用带小叉的蓝色小旗“ ”表示。

预定义计算机类型

除了检测代理扫描出来的计算机，管理员可以手工添加计算机，并为其指定类型，方便提前控制。选择“**操作->增加**”增加计算机，管理员可以设置 IP-MAC 对的类型，也可以只设置 IP 或 MAC 的类型。

设置类型	说明
IP-MAC	指定 IP 地址和 MAC 地址并设置类型，IP 和 MAC 唯一决定一个计算机，如果以后这个计算机被检测到，它的类型会自动更新为预先指定的类型；
IP	只根据 IP 地址指定类型，如果计算机记录包含该 IP 地址且没有指定类型，则会自动更新为该 IP 地址的类型； 假如设置 IP 地址 192.168.1.1 为授权，以后扫描到的计算机中，只要 IP 地址为 192.168.1.1，MAC 地址任意，则其类型自动为：IP 授权。
MAC	只根据 MAC 地址指定类型，如果计算机记录包含该 MAC 地址且没有指定类型，则会自动更新为该 MAC 地址的类型。 假如设置 MAC 地址 00-F0-4C-8C-DE-6A 为非法，则以后扫描到的计算机中，只要包含了这个 MAC 地址，其类型会自动更新为：MAC 非法

管理员可以增加计算机，指定部分 IP 地址或 MAC 地址为非法、授权或保护，则以后符合条件的计算机出现时，其类型会自动更新为预先设置的类型，检测

代理会根据类型控制这些计算机的访问权限。

查找和删除计算机

计算机记录太多，不方便查看时，管理员可以通过**“操作->查找”**来显示自己要查看的计算机列表，查找条件分 2 种：按 IP 地址范围和按最后出现日期范围查询。查询范围在接入检测窗口的状态栏中显示。

对于长久未使用的计算机，可以删除，如果该计算机再次出现，则列表中仍会再显示该计算机。

第十一章　数据备份

11.1使用数据库备份

主数据库备份

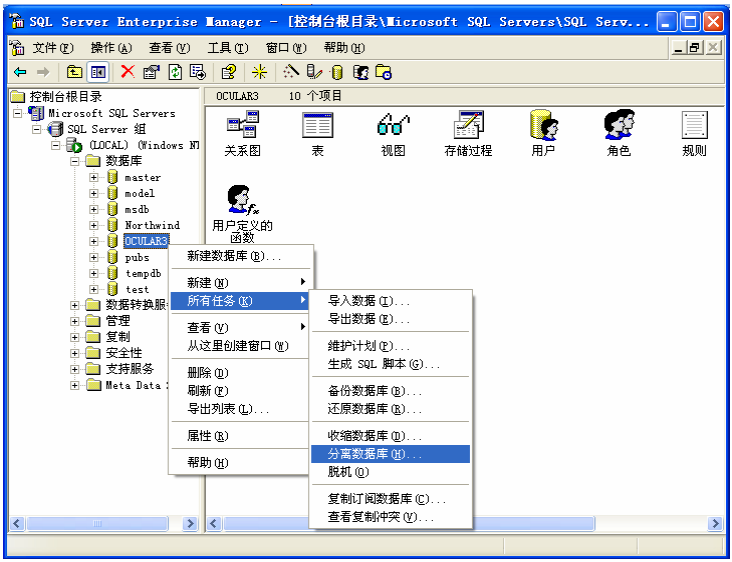
为了防止数据库文件破坏或其它意外情况造成服务器不能正常启动，建议管理员做好各种分类和策略后备份一下数据库文件。

主数据库的备份，主要操作下列步骤：

1) 首先停止 Viacontrol Server 以及其他一切使用 OCULAR3 数据库的程序；

2) 打开 SQL Server 2000 的企业管理器或 SQL Server 2005 的 Management Studio；

3) 右键点击“OCULAR3”数据库，选择菜单“**所有任务->分离数据库**”



4) 分离数据库成功后，管理员可以将主数据库文件 OCULAR3_Data.mdf、

OCULAR3_Log.LDF、
OCULAR3_SCREEN_Data.NDF、
OCULAR3_MAIL_Data.NDF、
OCULAR3_DOC_Data.NDF、
OCULAR3_PRINT_Data.NDF 共六个文件一起复制到备份目录下；

5) 分离完成后，企业管理器中的 OCULAR3 目录会被清除，管理员需要通过选择菜单“**所有任务->附加数据库**”还原 Server 安装目录下的主数据库。

上面是通过分离数据库然后复制数据库文件来备份的，也可以先把 MSSQLSERVER 服务停止，然后复制数据库文件到备份目录，再启动 MSSQLSERVER 服务和 Viacontrol 服务，同样可以达到备份的目的。

11.2控制台备份及查看

11.2.1 备份数据

管理员可以使用控制台提供的备份数据功能定期备份客户端的数据，将数据存放在其它盘符或移动存储设备中，以防止数据量太大，磁盘空间不足而引发的问题。

选择菜单“**工具->数据备份与查看**”打开备份数据与查看窗口。

创建备份任务

点击【数据库备份任务列表】右侧的创建按钮“ ”，新建一个新的备份任务，具体步骤如下：

1) 选择需要备份的数据的日期范围，设置起始时间和结束时间；

2) 选择需要备份的数据类型，包括：主要数据、文档、邮件和屏幕历史，其中主要数据是基本数据，是必选的，其他数据类型为可选；

3) 为了清理数据库空间，管理员可以勾选“**备份任务完成后删除已备份的数据**”自动清除已经备份的数据，否则备份的数据不会从主数据库中删除；

4) 删除已经备份的数据，数据库的大小不会变化，如果有需要，可以同时选中“**释放数据库空间**”，否则不会自动释放数据库空间；

5) 选择保存备份数据的路径；

6) 点击【确定】，启动备份任务。

备份任务列表

备份任务列表显示了备份任务的基本属性，包括：开始时间、结束时间、路径和状态。

字段名称	说明
开始时间 结束时间	备份任务的启动时间和备份完成的时间，由此可以得出备份任务完成所需要的时间；
路径	备份的数据文件所在的目录，包括了备份文件所在文件夹的名称，显示了备份数据的时间范围；
状态	正在备份中的任务状态是实时变化的，可以查看当前备份到了哪个表，状态还包括：已经取消、成功、失败等。

在备份任务列表里还可以做以下的操作：

图标按钮	操作
	停止备份任务，如果想取消当前的备份任务，可以单击【停止】按钮，停止当前的备份任务；
	查看备份任务条件，查看当前备份任务的详细设置；
	查看备份任务明细，查看该备份任务的详细日志。包括任务的启动，备份到了哪个表，备份完成的表，以及备份任务的成功，取消和失败原因等日志信息
	刷新备份任务列表

注意 备份任务只能同时执行一个，如果已经存在正在执行的备份任务则不能再增加新的备份任务。备份任务列表只能最多显示最近的 10 个备份任务。

11.2.2 加载和卸载备份数据

备份的数据不能直接查看，管理员需要将备份数据加载到数据库中才能查看。加载备份数据只是将备份的数据还原到服务器中，但并不破坏服务器现有的数据。

选择菜单“**工具->数据备份与查看**”打开数据备份与查看窗口，可以直接查看

已加载的备份数据列表，也可以加载和卸载备份数据。

加载备份数据

单击【已加载备份数据列表】右侧的【加载】按钮“ ”，选择备份数据文件所在的目录，单击【确定】加载指定的备份数据。

备份数据列表中显示了备份数据的起始日期、终止日期以及文件路径，最多可以同时加载 12 个备份数据。

加载了的备份数据可以直接通过控制台查看以及查询，不会影响服务器中本身数据的查看。

卸载备份数据

假如不需要查看某个备份数据，也可以将备份数据从服务器中卸载。选择需要卸载的备份数据，单击【卸载】按钮“ ”，对应的备份数据列表将被删除，在控制台上也不能再查看到这些备份数据。

第十二章　工具

12.1账户管理

系统管理员具有最高权限，他可以使用系统内的所有功能。系统管理员可以通过新建管理员的方式来使其他的管理者执行某些管理功能。

选择菜单“**工具->账户**”，系统管理员可以查看和添加新的管理员。

图标按钮	操作
	添加管理员帐号，也可输入描述信息；
	删除管理员帐号，系统管理员“Admin”无法删除

管理员管理权限拥有四大模块。包括：常规，权限，计算机和用户范围。

管理权限	内容
常规	指定管理员的类型，管理员登录的模式等；
权限	指定非系统管理员账户拥有的权限；
计算机/用户组	指定非系统管理员所能管理的范围，计算机组和用户组只能指定其中一种，假如指定了计算机组，就不能指定用户组；如果指定全部计算机组，则默认也是全部用户组。

管理员的功能权限

功能权限	说明
文件	主要是对计算机树与用户树的操作的权限，如：新建组，移动，重命名，删除等。同时也包括导出数据与打印。
控制	主要是对客户端控制的权限。 包括：锁定/解锁，发送通知消息， 注销计算机帐户，开机/关机，远程唤醒，卸载客户端。
统计	主要是对统计记录查询的权限。 包括：应用程序统计，上网浏览统计，网络流量统计等。
日志	主要是对日志记录查询的权限。 包括：基本日志，应用程序日志，上网浏览日志，文档操作日志，共享文档日志，文档打印日志，资产变更日志，策略日志，系统日志，备份文档，移动存储日志。
策略	主要是对策略查询与修改的权限。 包括：基本策略，应用程序策略，上网控制策略，设备控制策略，打印控制策略，屏幕记录策略，日志记录策略，远程控制策略，流量控制策略，端口控制策略，邮件控制策略，IM 文件控制策略，上传下载控制策略，文档控制策略，系统报警策略，移动存储授权策略。
监控	主要是对屏幕，邮件，即时通讯等记录进行查询与导出等操作的权限。 包括：查看实时屏幕，查看邮件记录，查看即时通讯记录，查看屏幕历史，导出屏幕历史等。

功能权限	说明
维护	主要是对远程计算机进行维护操作的权限。 包括：查看远程信息，控制远程信息，远程控制，远程文件传送等。
资产管理	主要是对资产进行管理的权限。 包括：查看资产信息，设置资产类别属性，修改自定义类别与属性等。
补丁管理	主要是对系统补丁进行管理的权限。 包括：查询补丁信息，设置补丁参数，执行补丁安装。
漏洞管理	主要是对系统漏洞进行管理的权限。 包括：查询漏洞检查情况，设置漏洞检查参数等。
软件分发	有两部分，对分发包操作的权限。 包括：查询分发包，设置分发包等；对分发任务操作的权限。包括：查询分发任务及安装情况，设置分发任务，执行分发任务等。

功能权限	说明
网络接入检测	主要是接入检测功能的权限。 包括：查看接入检测、设置接入检测和设置策略。
类别管理	主要能管理的类别的权限。 包括：应用程序类别，网站类别，时间类别，网络地址类别，网络端口类别和移动存储库。
删除操作	主要是指定能删除哪些记录的权限。 包括：统计，日志，邮件，即时通讯的删除。
备份数据	主要是备份数据与查看数据的权限。 包括：备份日志，查看数据
参数设置	主要是设置搜索范围和排除范围的权限。 包括：设置客户端的搜索范围、设置客户端的排除范围。
生成客户端确认码	是指生成客户端确认码的权限。
管理加密盘	主要包括：设置分类，设置策略等。
格式化为加密盘	如果选择了该项，则管理加密盘的权限会自动勾选，对加密盘有完全的控制权限。

管理员在设置安全权限的时候根据实际需要出发，不要赋予不应该的权限。

12.2计算机管理

为了便于管理员对整个网段安装了客户端模块的计算机进行管理，也方便用户可以查询 license 的使用情况，比如查询现在使用了多少个 license，是否超出了 license 范围等，我们可以通过计算机管理来查看这些情况。

选择菜单“**工具->计算机**”进入计算机管理查看窗口。

计算机列表中包含的内容有：

属性名称	说明
	该图标表示计算机在 license 范围内，属于授权的计算机，没有这个标志的计算机超出了 license 范围，请通过“**授权信息**”查看购买的 license 和当前使用的 license 数量。
名称	客户端计算机在控制台上显示的名称；
计算机	客户端计算机的名称；
ID	服务器为客户端分配的 ID，唯一标志该计算机；
网络地址	客户端使用的 IP 地址；
网卡地址	客户端的网卡地址和 IP 地址；
所属分组	客户端所属的计算机分组；
首次出现时间	客户端第一次出现的时间；
最后出现时间	客户端最后一次出现的时间；
版本	客户端的版本信息；
安装时间	客户端的安装时间。

管理员可以根据查询条件快速查找需要查看的计算机信息，查询条件包括：

查询条件	说明
全部	默认查询所有安装了客户端模块的计算机；
按 IP 地址	设置 IP 地址范围，查询指定范围内的客户端机器；
按首次出现日期	设置日期范围，查询首次出现日期包含在该范围内的客户端机器；
按最后出现日期	设置日期范围，查询最后出现日期包含在该范围内的客户端，方便查找已经一段时间没有出现的客户端；
按客户端 ID	根据客户端 ID 查询指定的一个客户端信息；
按计算机名称	按名称查询，支持模糊查询。

管理员可以选中一个或多个计算机，进行“**删除**”或“**卸载**”的操作来管理自己的 license。

操作	说明
删除	管理员可以删除不需要的客户端来释放 license 数量，删除会在卸载客户端的同时减少 license 数量；
卸载	卸载客户端不会减少 license 数量。

执行了删除或卸载的操作后，管理员必须单击【确定】按钮对改动进行确认，否则所做的操作将不生效。这样做的目的也是为了减少失误。

12.3警报信息

警报信息记录了所有策略触发的实时报警日志，在“**工具->警报**”中查看。如果控制台设置了“弹出报警气泡”，当有客户端触发了某个策略后，会在控制台机器上弹出报警气泡，通过点击报警气泡查看所有的实时报警记录。

实时报警默认最多能显示 500 条记录，管理员可以通过“**工具->选项->实时报警->报警窗口**”来调整实时报警窗口能够显示报警记录的最大数量。

警报信息记录的是实时报警，关闭控制台或重新登录控制台报警记录会自动清空。如果管理员需要查询，请到“**日志->策略日志**”中查询。

12.4分类管理

为了方便查询、统计和设置策略，管理员可预先在系统中设置好分类，分类管理包括：应用程序分类、网站分类、移动存储分类、时间类型分类、网络地址分类和网络端口分类。

12.4.1 应用程序分类

选择“**工具->分类管理->应用程序**”打开应用程序类别窗口，系统默认定义了两个应用程序类别：系统应用程序和未分类。

“系统应用程序”分类是指与操作系统相关的一些程序，为了避免严重问题，将这些系统程序分离开来，单独放在该分类，管理员也可以根据需要移动其它的程序到该分类。

所有的应用程序都是在客户端搜集到的，如果没有匹配到任何分类则被归类为“未分类”。管理员可以新建其它分类并将相关程序从“未分类”移动到新建的分类，但是不能手工增加应用程序。

管理员根据企业管理的需求将类型相同的应用程序放在一个类别，对于分类的操作包括：

操作	说明
新建分类	在应用程序类别根目录，选择“**操作->新建**”或单击右键“**新建**”增加一个新类别并输入类别名称；在一个类别中也可增加子分类，选择该分类，单击右键“**新建**”则在该分类中新建一个子分类；
移动应用程序	增加了分类，需要将相关的程序都移动到该分类，找到相关程序，右键“**移动到**”指定目标分类进行转移，或按住鼠标左键拖拽到指定分类； 可同时选中多个应用程序进行转移，按住 Ctrl 键或 Shift 键进行多选；
查找	选择“**操作->查找**”可以查找指定的应用程序及所在分类，可以按应用程序的名称、文件名称和描述进行查找，输入的内容满足这 3 个属性的中任意一个均可。 查找功能也可用于快速分类，比如需要将所有 QQ 程序移动到 QQ 分类，可以在查找中输入内容“qq”，则会查询所有的 qq 程序，然后将查询的结果一起拖拽到 QQ 分类，这样大大方便了管理员的分类工作。

注意 未分类和系统应用程序类别都不能删除，也不能创建子类别。

12.4.2 网站分类

管理员可以根据企业需要，将网站进行分类，方便管理员按照类别统计和控制员工的上网浏览情况。

点击“**工具->分类管理->网站**”打开网站类别窗口，系统默认分类为空，管理员需要手工添加网站类别库和网站识别，网站识别支持通配符。

操作	说明
新建分类	在左侧的网站类别视图选择“**操作->新建->网站类别**”新建网站类别并命名；也可在一个分类下面新建一个子分类；
新建网站识别	建好分类后，在右侧的网站视图单击右键“**新建->网站识别**”增加一个网站识别并输入名称和网址，网址的输入可以是完整的网址，也可以支持通配符“*”“？”等，如：*sina*，*game*等；
查找	选择“**操作->查找**”或单击工具栏上的查找按钮 可以查找指定的网站属于哪个分类或是否存在，查找支持模糊查询。

12.4.3 移动存储分类

为了方便管理企业内部移动存储盘的使用，我们需要在移动存储库中首先对企业内部所有使用的移动存储盘进行分类。管理员可以把属于一个部门或者个人使用的移动存储盘放在一个分类，然后对这些分类的存储盘授予不同的权限，以防止资料的泄露。

移动存储盘可以分为加密盘和非加密盘（普通盘），加密盘是指经过我们产品加过密的移动盘，只能在客户端机器上正常使用，没有安装客户端的机器无法使用该盘，加密盘只能通过控制台来制作。

选择“**工具->分类管理->移动存储**”打开移动存储库窗口，系统默认有一个“未分类”类别。管理员可以手工添加新类别。

移动存储信息的获取

移动存储信息的获取主要有 2 种方式：

获取方式	说明
客户端获取	所有在客户端机器上使用过的移动存储信息都会放在未分类中，管理员可将这些移动存储移动到其它自定义分类。客户端只能获取普通存储盘信息；
控制台获取	管理员可将移动存储直接插入控制台机器来添加移动存储信息，选择“**操作->本地移动存储信息**”查看插入的移动存储信息，其中有标志“ ”的表示该移动存储还没有保存在移动存储库中：
	手工刷新本地移动存储列表；
	设置移动存储分类，，第一次插入的盘默认放在“未分类”，单击该按钮，可以选择其它分类进行存放；
	保存按钮，将移动存储信息保存到分类库；
备注	为移动存储添加备注信息，方便管理员查看和识别。

制作加密盘

管理员将需要整盘加密的移动盘依次插入控制台的机器上，制作加密盘。选择“**工具->分类管理->移动存储**”打开移动存储库，选择菜单“**操作->本地移动存储信息**”查看本地移动盘列表。

按图标按钮“ ”将正常的移动盘格式化为加密盘。格式化为加密盘后，该盘

上的所有文件将被删除，并且将只能在安装了本产品客户端的机器上使用，请管理员确认是否执行格式化操作。

格式化成功后，图标将变为“ ”，表示该盘是加密盘，但还没有保存，单击保存按钮后，图标变为“ ”。

注意 只有拥有正式产品序列号的产品才有加密盘的功能，否则该按钮为灰色，不可用。

加密盘格式化为非加密盘

管理员也可以将加密盘还原为普通盘，也就是非加密盘，格式化加密盘为非加密盘的方法有 2 种：

在没有安装客户端的机器上手工格式化

1. 加密盘在客户端机器上可以正常打开并且使用，而在没有安装客户端的机器上打开时，会提示需要格式化。如果用户选择了“是”，将手工格式化该盘为非加密盘，同时删除该盘上的所有文件。
2. 对于管理严格的企业，需要提醒员工谨慎操作，如果手工格式化之后，就不再是加密盘了。

通过控制台将加密盘格式化为普通的盘

在控制台机器上插入加密盘，打开移动存储库，查看本地移动存储信息，可以看到该加密盘信息。

选中加密盘，按图标按钮“ ”，格式化该盘为非加密盘，格式化成功后，该盘的图标又变回“ ”，并且序列号发生变化，需要重新保存；

加密盘不能通过常规的 Windows 的右下角的即插即用的设备里进行安全拔出，如果需要拔出加密盘，单击该界面中的拔出按钮“ ”后，可以安全拔出该加密盘。

注意 在客户端机器上使用加密盘时，需要单击加密盘后右键选择“Eject device”安全退出。

移动存储的属性说明

移动存储设备包括 U 盘、移动硬盘、记忆棒、智能卡等可移动设备。移动存储的属性内容包括：

属性名称	说明
序列号	每一个可移动设备都有一个序列号，序列号是一个移动存储设备的唯一标识信息。
设备描述	对这个移动存储的描述信息。
备注信息	为了方便查看和区分移动盘，可以添加一些注释信息，默认为空，单击右键“**修改备注**”输入备注信息，比如：使用者，资产编号等。
卷容量	该移动存储盘的容量大小。
分区格式	该移动存储盘的分区格式，一般为：FAT，FAT32，NTFS。
类型	是否为加密盘，类型为空表示为普通盘（非加密盘）
卷标	移动存储盘的卷标。
查看使用情况	双击移动存储信息可以查看其详细属性，点击【查看使用情况】按钮可以查看该盘的使用情况，确定该存储盘的使用范围。或直接右键单击一条存储信息选择“**查看使用情况**”查看该存储盘的使用情况。

查找

移动存储库提供了多种查询条件以方便管理员查找需要的移动存储信息，选择“**文件->查找**”或直接点击工具栏上的【查找】按钮“🔍”打开查询框：

查找条件	说明
卷序列号	按卷序列号进行查询，输入指定的卷序列号，这里不支持模糊查询，需要输入完整的序列号；
类别	默认是全部分类，也可以指定其中部分类别进行查询；
描述	按移动盘的描述信息进行查询，支持模糊查询，比如输入 usb，则查询出的结果中设备描述包含 usb；
卷标	不输入任何任务代表全部，输入卷标如 h 进行查询；
分区格式	按照分区格式进行查询，如输入 NTFS 查询分区格式为 NTFS 的所有移动盘信息；
备注	根据备注信息进行查询，支持模糊查询；
卷容量	设置一个卷容量的范围，按移动盘的卷容量进行查询。

管理员可设置多个查询条件，进行更精确的查询，查询的结果中包含了移动盘所属的类别信息，管理员可以拖动移动盘信息到指定的类别。

12.4.4 时间类型分类

为查询和统计的方便，管理员可以预先定义好时间段类别。点击“**工具->分类管理->时间类型**”，管理员可以查看现有时间类别。系统默认有四种时间类型：全天，工作时间，休息时间，周末时间。

管理员可以根据企业工作时间去修改这些时间类型，点击一种时间类型，查看时间范围并且对其编辑修改。除了系统定义好的时间类别，管理员可以添加其它时间类别。

操作	说明
添加时间类型	单击该增加按钮“”增加一个新类别并且输入类别名称，时间范围默认是全天，需要手工编辑修改时间段。
删除时间类型	选择需要删除的时间类别，单击删除按钮“”删除时间类型，系统默认的四个时间类型不能删除。

12.4.5 网络地址分类

点击“**工具->分类管理->网络地址**”，管理员可以预定义网络地址类别。系统默认定义了全部，企业网，互联网，局域网和外网。因局域网和外网不可修改，因此在分类管理里无法查看到。

系统会根据服务器 IP 地址自动生成企业网的地址范围，管理员可以修改为企业内部网络的 IP 地址范围，系统会自动生成互联网的 IP 地址范围（除了企业网的 IP 范围之外的 IP 都属于互联网范围）。除了系统定义的地址类别，管理员还可以手工添加新类别，并输入该类别的 IP 地址段。

注意 在网络地址类别中，不能查看局域网和外网，但是在网络流量统计、流量控制策略和网络控制策略中可以看到局域网和外网。实际上，局域网是对单个计算机来说的，是指该计算机所在的网段；外网是相对于局域网来说的。

12.4.6 网络端口分类

点击“**工具->分类管理->网络端口**”，管理员可以预定义端口类别。系统默认定义了全部，ICMP，TCP，UDP，邮件，网页，网络共享这些类别。其中，全部、ICMP、TCP、UDP 的类别不可添加和修改内容，邮件、网页、网络共享的端口范围可以添加和修改。

除了系统定义的这些常用端口类别，也可以手工添加新的端口类别及其端口范围。系统定义的端口类别无法删除和重命名，而手工添加的端口类别可以删除和重命名。

12.5服务器管理

选择“**工具->服务器管理**”，管理员可以通过控制台查看服务器的信息，包括：基本信息、数据库文件信息、目录信息、磁盘空间信息。

服务器信息	说明
基本信息	包括服务器的开机时间，服务器的运行时间，实时流量；
开机时间	服务器最后一次的启动时间；
运行时间	服务器启动后一共运行的时间；
流量	服务器与客户端之间发送、接收数据的实时流量；
数据库文件信息	数据库文件的名称，路径和文件大小；
目录信息	屏幕历史、邮件、备份文档、软件分发和微软补丁的目录信息，包括名称、路径目录文件数量及文件大小；
磁盘空间信息	服务器所在的计算机的磁盘信息，包括盘符、文件系统、容量、空闲空间以及磁盘使用率。

12.6客户端工具

确认码计算器

当安装了客户端的计算机无法连接服务器，例如禁用网卡或出差时，而又临时需要解除策略或者卸载客户端，这时是无法通过控制台去设置相应的策略的。

用户可以直接在客户端机器上调用客户端工具，具体操作步骤：

1) 在客户端机器按住“Ctrl+Alt+Shift”，然后依次输入“oculara t”字符串，打开客户端工具；

2) 选择“清除所有策略”，点击【生成操作码】按钮；

3) 会弹出一个“检验操作码”对话框，用户需要把原始操作码报告给管理员；

4) 管理员在控制台“**工具-客户端工具-确认码生成器**”输入客户端的操作

码，会解析出该客户端的操作以及相应的客户端信息；

5) 管理员确认后点【生成确认码】；

6) 管理员将确认码告诉客户端，输入正确的确认码继续执行指定的操作。

使用客户端工具卸载客户端的详细说明请参考前面“第二章 Viacontrol安装和部署->2.6 卸载 Viacontrol->2.6.2 卸载客户端”。

12.7选项

选择“**工具->选项**”，管理员可以查看并修改当前控制台和服务器的缺省值。

12.7.1 控制台参数设置

控制台参数里可以设置日志查看，实时信息和实时报警的参数：

参数	说明
日志查看	
日志查询	查询每页显示的最大数量，系统默认为每页 20 条；
实时信息	
监视	实时屏幕跟踪时间间隔，系统默认为 2 秒；
实时维护	应用程序列表跟踪时间间隔，系统默认为 2 秒； 进程列表跟踪时间间隔，系统默认为 2 秒； 性能列表跟踪时间间隔，系统默认为 2 秒；
实时报警	
报警窗口	报警窗口显示记录的数量，系统默认为 500 条；
气泡设置	弹出报警气泡：勾选后在此控制台的机器上会弹出因策略触发的实时报警。 弹出气泡的最低警报级别：低，重要，严重

12.7.2 服务器参数设置

服务器参数里可以设置多个系统参数：

参数	说明
补丁选项	
新出现的客户端默认自动安装	勾选此项，新安装客户端的计算机会自动安装已经下载的补丁，否则新客户端机器不会自动安装补丁。如果需要客户端自动安装补丁，管理员可以在第一次登录控制台时设置该项；
新发现的补丁默认自动下载	勾选此项后新扫描到的补丁会自动下载，否则新扫描到的补丁不会自动下载。如果需要所有扫描出来的补丁自动下载，管理员可以在第一次登录控制台时设置该项；
数据清除	
清除选项	该选项可以设置各种日志数据的保留时间，设置范围：5-180 天，设置了清除范围后，服务器会自动删除之前的数据。如果数据量很大而又不需要全部保存，就可以设置自动清除数据； 包括的数据类型有：基本事件、文档操作、网页浏览、应用程序、资产变更、打印、共享文档操作，策略日志、系统日志等日志数据以及历史屏幕、即时通讯、邮件、应用程序统计、网页浏览统计、网络流量统计等数据；
管理范围	
搜索范围	可以添加服务器搜索客户端机器的 IP 地址范围，一般用于客户端无法主动连接正确的服务器，服务器应开启主动轮询功能；
排除范围	可以添加服务器的排除客户端机器的地址范围。在排除范围内的客户端不能与该服务器连接；
连接设置	
服务器和客户端之间的带宽设置	带宽设置范围是 1-102400 KB/s，在局域网内一般不用限制带宽，对于 VPN 网络可能会用到；
主动轮询	服务器会按照处于 license 范围内的客户端列表主动连接客户端的 8235 端口，默认开启。不勾选此项，服务器不会主动去连接客户端；

参数	说明
目录设置	
数据目录	管理员可以更改一些数据文件的存放路径，包括：软件分发、备份邮件、屏幕历史、备份文档、微软产品补丁。 默认的保存目录是 Viacontrol 安装目录；管理员可以修改这个目录，但是之前的数据不会自动移动到新的目录中，需要停止服务器然后手动移动数据到新目录。新目录设置后必须重启服务器才生效。
设置目录	点击设置按钮“ ”打开服务器计算机的目录树，选择新的数据存放目录，直到重启服务器后，保存目录才会更新为新目录；
恢复初始目录	点击恢复按钮“ ”，将指定数据对象的保存目录恢复到初始的目录，初始的目录是服务器模块的安装目录；
性能设置	
固定模式	固定模式是设置服务器能并发处理客户端的最大数量，设置的范围是[0-100]；
动态模式	动态模式是服务器自动根据负载调整并发处理客户端得数量。负载级别“标准”表示服务器模块对于数据库进程的平均占用率是 30%；如果是“高”，这个上限值是 50%，如果是“低”，这个上限值是 10%。； 服务器默认是在动态模式下运行，处理模式是“标准”； 一般来说，在动态模式下，服务器的性能越好，并发处理的客户端数量会越多。 对于实时性的操作，如控制台查看实时屏幕，或者进行远程维护等，不受这个选项的影响，会实时处理。
报错设置	
记录验证客户端过程中的报错信息	勾选该项才会记录报错信息，服务器的报错信息可在“**日志->系统事件**”里查看；
记录报错信息的最低别	级别是指报错信息的严重度： 全部 报告全部的错误； 低　通讯中客户端的回应并不是预期的结果； 中等 超过 license 授权； 重要 序列号或者检验码错误； 严重 因为处于服务器排除范围内而无法通过服务器校验

第十三章 审计控制台

审计控制台主要是对管理员操作控制台的一种日志记录，方便查询管理员在控制台上做过什么操作。

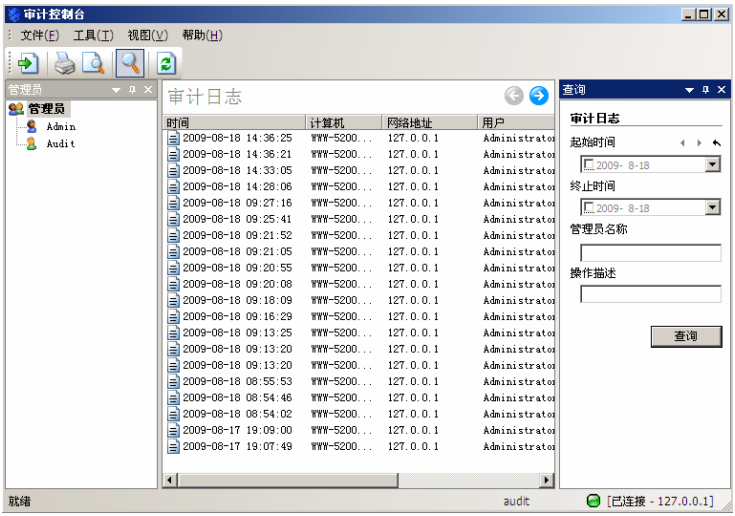
13.1登录审计控制台

单击安装目录下的 OConsole3.exe 或者“**开始->所有程序->Viacontrol V3-> Viacontrol V3 控制台**”启动控制台模块。

输入服务器 IP 或服务器机器名称，使用系统审计员的帐号“**audit**”，初始密码为空，登录到审计控制台。

13.2审计界面简介

审计控制台包括：标题栏、菜单栏、工具栏、管理员栏、数据视图、查询栏和状态栏。



管理员栏显示的是所有管理员和审计员的列表，选择其中一个管理员，则审计日志将显示该管理员的所有操作日志。

审计日志视图提供了打印、导出功能以保存有用的统计日志，也提供了删除功能以便删除无用的审计日志。

字段名称	说明
打印/打印预览	选择菜单“**文件->打印/打印预览**”打印当前的审计日志；
导出	选择菜单“**文件->导出**”导出审计日志，导出有 2 种方式，右键“**导出->本页记录**”、“**导出->所有满足条件的记录**”；
删除	选择菜单“**文件->删除**”删除审计日志，删除有 3 种方式，单击右键“**删除->选中的记录**”、“**删除->本页记录**”、“**删除->所有满足条件的记录**”。

13.3使用审计控制台

审计日志内容

审计日志包括控制台登录情况，管理员的操作日志、修改删除策略、查看实时屏幕、远程控制、设置管理员的账户与权限等。

审计日志记录的内容包括：

字段名称	说明
时间	管理员操作控制台的具体时间；
计算机	管理员登录控制台所在的计算机名称；
网络地址	管理员登录控制台所在计算机的 IP 地址；
管理员	管理员的账户名称；
描述	管理员对控制台的操作描述信息。

审计日志查询

审计管理员可以通过时间范围、管理员名称、操作描述来查询需要的日志信息。

查询条件	说明
时间范围	设置一个时间范围，查询一个时间段内的审计日志；
管理员名称	查询指定管理员的审计日志，管理员列表在管理员栏中查看；
操作描述	根据审计日志的描述信息查询指定操作的审计日志。

设置审计员账户

选择菜单“工具->账户”，系统审计员可以查看和添加新的审计员账户并设置其功能权限。

字段名称	说明
常规	指定审计员的类型，审计员登录的模式等。与控制台管理员账户设置的意义相似；
功能权限	功能权限包括审计日志的保存及删除；
文件	包括导出数据和打印的权限；
删除	是指删除日志数据的权限。
管理对象	选择该审计员可以审计的管理员，使该审计员有权限查

	看选择的管理员的操作日志；可同时选择多个。系统审计员可以审计所有的管理员。

技 术 支 持

感谢您对我们产品的支持和信赖，为客户提供优质的技术支持是我们的承诺。如果您有任何本手册无法解决的技术问题请发电子邮件到我们的技术支持部门，我们将尽快回答您的问题：

hupu@hupu.net

您也可以直接致电我们垂询：

电话（上海）：+86-21-51028848

传真（上海）：+86-21-51069353

您的意见和建议对我们很重要，我们会根据您的建议对我们的产品不断地进行改进。

HUPU　Information Technology
互普信息技术